



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/OPS/DP/POLCY/2023/411

July 14, 2023

MASTER CIRCULAR FOR DEPOSITORY PARTICIPANTS (DPS)

1. The Depositories Act 1996 ("the Act"), the SEBI (Depositories and Participants) Regulations, 2018 ("the SEBI Regulations"), the Bye-Laws of CDSL ("Bye-Laws"), Operating Instructions of CDSL ("Operating Instructions"), the various Circulars issued by SEBI and various Communiqués issued by CDSL provide the framework for the depository and depository participants to fulfil certain compliances relating to functions in the depository system.
2. SEBI vide its Circular No. SEBI/HO/MRD/POD 3/ CIR/P/2023/58 dated April 20, 2023 has instructed depositories to issue the Master Circular consolidating all guidelines issued and applicable as on March 31 of every year, segregated subject-wise. SEBI has also directed that such Master Circular shall not include Bye-Laws, Rules (ie Operating Instructions in case of CDSL) and Regulations issued by Market Infrastructure Institutions (MIIs), Status of any compliance by the market participant and actions taken against any entity.
3. Accordingly, this Master Circular is a compilation of the relevant Communiqués pertaining to DPs issued by CDSL up to March 31, 2023. The guidelines forming part of Bye laws and Operating instructions are not covered in the Master Circular. The user shall read the provisions mentioned in the Master Circular in concurrence with the relevant provisions of the Bye-Laws and Operating Instructions. In case of any inconsistency between the Master Circular and the applicable communiqués, users may refer to the detailed contents of the applicable/ relevant communiqué.
4. This Master Circular consists of 17 Chapters and shall come into force from the date of its issue. Efforts have been made to include provisions of the communiqués/ communications relevant to each section. However, cross referencing of communiqués/communications amongst the chapters may exist. Users may refer other chapters also for compliance towards provisions/guidelines applicable to them. References in the Master Circular to the provisions/guidelines which now stand repealed, have been suitably updated. For ease of reference, each chapter of this circular contains footnotes corresponding to the respective circulars.



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

5. *“Notwithstanding such rescission,*
- a. *Anything done or any action taken or purported to have been done or contemplated under the rescinded guidelines before the commencement of this Master Circular shall be deemed to have been done or taken or commenced or contemplated under the corresponding provisions of the Master Circular or rescinded guidelines whichever is applicable.*
 - b. *The previous operation of the rescinded guidelines or anything duly done or suffered thereunder, any right, privilege, obligation or liability acquired, accrued or incurred under the rescinded guidelines, any penalty, incurred in respect of any violation committed against the rescinded guidelines, 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 guidelines have never been rescinded.”*

DPs are advised to take note of the same.

Queries regarding this communiqué may be addressed to CDSL – Helpdesk: at helpdesk@cdslindia.com and / or on telephone number 08069144800.

sd/-

Nayana Ovalekar

Chief Regulatory Officer



Central Depository Services (India) Limited

Convenient ⇌ Dependable ⇌ Secure

Master Circular

March 2023



Table of Contents

Chapter No.	Particulars	Page No.
	LIST OF ABBREVIATIONS USED	1
1	ACCOUNT OPENING	4
2	ACCOUNT MODIFICATION	36
3	DEMATERIALISATION	39
4	SETTLEMENTS	40
5	STATEMENT OF ACCOUNTS	53
6	PLEDGE	54
7	FREEZE / UNFREEZE	55
8	ACCOUNT CLOSURE	58
9	MUTUAL FUND UNITS	61
10	INTERNAL CONTROLS / REPORTING TO CDSL	63
11	GRIEVANCE REDRESSAL	82
12	MAINTENANCE OF WEBSITE BY DP	86
13	DP BRANCHES/SERVICE CENTRES	87
14	PREVENTION OF MONEY LAUNDERING ACT, 2002 (PMLA)	88
15	CYBER SECURITY AND CYBER RESILIENCE FRAMEWORK	97
16	IMPLEMENTATION OF THE MULTILATERAL COMPETENT AUTHORITY AGREEMENT (MCAA) AND FOREIGN ACCOUNTS TAX COMPLIANCE ACT (FATCA)	109
17	MISCELLANEOUS	110
	LIST OF RESCINDED COMMUNIQUÉS	114



LIST OF ABBREVIATIONS USED

Abbreviation	Term
AI	Artificial Intelligence
AMC	Asset Management Company
AML	Anti-Money Laundering
AOF	Account Opening Form
AOP	Association Of Persons
BCP	Business Continuity Plan
BO	Beneficial Owner
BSDA	Basic Services Demat Account
CAF	Common Application Form
CBDT	Central Board of Direct Taxes
CBS	Core Banking Solution
CC	Clearing Corporation
CDD	Client Due Diligence
CDSL	Central Depository Services (India) Limited
CEO	Chief Executive Officer
CERSAI	Central Registry of Securitisation Asset Reconstruction and Security Interest of India
CFT	Combating the Financing of Terrorism
CISA	Certified Information Systems Auditor
CISM	Certified Information Securities Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CKYCR	Central KYC records Registry
CM	Clearing Member
CMFA	Client Securities Margin Funding Account
CMR	Client Master Report
CRS	Common Reporting Standards
CSC	Client of Special Category
CSGL	Constituents' Subsidiary General Ledger
CSIRT	Computer Security Incident Response Team
CSP	Communications Service Provider
CUSA	Client Unpaid Securities Account
CUSPA	Client Unpaid Securities Pledgee Account
DDP	Designated Depository Participant
DDPI	Demat Debit and Pledge Instruction



Abbreviation	Term
DIS	Delivery Instruction Slip
DP	Depository Participant
DRF	Dematerialisation Request Form
DRN	Demat Request Number
ECS	Electronic Clearing Service
FATCA	Foreign Accounts Tax Compliance Act
FATF	Financial Action Task Force
FEMA	Foreign Exchange Management Act
FII	Foreign Institutional Investor
FIU	Financial Intelligence Unit
FPI	Foreign Portfolio Investor
GC	Global Custodian
GRC	Grievance Redressal Committee
HUF	Hindu Undivided Family
IGRP	Investor Grievance Resolution Panel
IPF	Investor Protection Fund
IPV	In Person Verification
IRDAI	Insurance Regulatory and Development Authority of India
ISACA	Information Systems Audit and Control Association
ISC	Investor Service Centre
ISF	Investor Service Fund
ISIN	International Securities Identification Number
IVRS	Interactive Voice Response System
KMP	Key Managerial Personnel
KRA	KYC Registration Agency
KUA	e-KYC User Agency
KYC	Know Your Client
LLP	Limited Liability Partnership Firm
MCAA	Multilateral Competent Authority Agreement
MD	Managing Director
MICR	Magnetic Ink Character Recognition
ML	Machine Learning
MPIF	Margin Pledge Invocation Form
MPRF	Margin Pledge Request Form
MPSN	Margin Sequence Number
MURF	Margin Unpledge Request Form



Abbreviation	Term
NAV	Net Asset Value
NCIIPC	National Critical Information Infrastructure Protection Centre
NISM	National Institute of Securities Markets
NRI	Non-Resident Indian
OCB	Overseas Corporate Body
OVD	Officially Valid Document
PAN	Permanent Account Number
PFRDA	Pension Fund Regulatory and Development Authority
PMLA	Prevention of Money Laundering Act
PMS	Portfolio Management Services
POA	Power Of Attorney
PRF	Pledge Request Form
QFI	Qualified Foreign Investors
RBI	Reserve Bank of India
RE	Regulated Entities
RGESS	Rajiv Gandhi Equity Savings Scheme
ROC	Registrar Of Companies
RRF	Rematerialisation Request Form
RRN	Rematerialisation Request Number
RTA	Registrar & Transfer Agent
SCORES	SEBI Complaints Redress System
SEBI	Securities & Exchange Board of India
SOA	Statement of Accounts
SOC	Security Operations Centre
SOP	Standard Operating Procedure
STR	Suspicious Transaction Report
TM	Trading Member
TPIN	Transaction Personal Identification Number
TRF	Transmission Request Form
TRPF	Transposition Request Form
UCC	Unique Client Code
UIDAI	Unique Identification Authority of India
URF	Unpledge Request Form
VAPT	Vulnerability Assessment and Penetration Tests
VIPV	Video in Person Verification



Chapter 1 : Account Opening

1.1 Unique Mobile Number and Email ID¹

- 1.1.1 Depository Participants are advised to ensure that separate mobile number and e- mail address is uploaded for each client. However, under exceptional circumstances, the Participants may, at the specific written request of a client, upload the same mobile number/E-mail address for more than one client provided such clients belong to` one family. ‘Family’ for this purpose would mean self, spouse, dependent children and dependent parents.

1.2 Bank Details

- 1.2.1 DPs should note that bank account details of PMS should not be captured in place of bank account details of clients in depository system, in case of PMS accounts.²

1.3 Rights and Obligations of the Beneficial Owners and Depository Participant³

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to Rights and Obligations of the Beneficial Owners and Depository Participant shall require to be complied with:

- 1.3.1 The DP shall ensure that any clause in any voluntary document neither dilutes the responsibility of the DP nor it shall be in conflict with any of the clauses in this Document, Rules, Bye-laws, Regulations, Notices, Guidelines and Circulars issued by SEBI and CDSL from time to time. Any such clause introduced in the existing as well as new documents shall stand null and void.
- 1.3.2 The DP shall make available this document to the clients, either in electronic or physical form, depending upon the preference of the client as part of account opening kit. In case the document is made available in electronic form, DP shall maintain the logs of the same. It is also reiterated that DPs shall continue to make the aforesaid document available on their website and keep the clients informed about the same.⁴

¹ Reference: CDSL/OPS/DP/POLCY/5139 dated April 15, 2015

² Reference: CDSL/OPS/DP/1931 dated March 22, 2010

³ Reference: CDSL/OPS/DP/ POLCY/4095 dated December 04, 2013

⁴ Reference: CDSL/OPS/DP/POLCY/6029 dated July 18, 2016



1.3.3 The DP can obtain the acknowledgement in any one of the following ways:⁵

- (a) On a separate form of acknowledgment stating that they have received the ‘Rights and Obligations document’;
- (b) On a register maintained for this purpose;
- (c) Can incorporate the acknowledgement as a part of the Account Opening Form. In this case the signatures of the BOs is not required to be taken again;
- (d) Can obtain an acknowledged copy of the ‘Rights and Obligations document’ where the BOs can sign only on the last page of the document;
- (e) Can affix a stamp on the account opening form stating that ‘I/We have received and read the copy of Rights and Obligations document’ and obtain signature of all the holders against the same separately.

1.3.4 Signature of all the holders is required on the acknowledgement of the ‘Rights and Obligations document’.

1.3.5 The POA holder of an individual BO cannot give acknowledgement of the receipt of the ‘Rights and Obligations document’. For non-individual / corporate accounts the authorized signatories shall acknowledge the receipt of the ‘Rights and Obligations document’.

1.3.6 In case of a client proposing to open multiple demat accounts, each demat account is treated as a different BO and hence separate ‘Rights and Obligations document’ has to be provided and acknowledgement obtained for each account separately.

1.4 Mandatory updation of certain Attributes of KYC of Clients⁶

1.4.1 DPs are advised to take note of the details of 6 KYC attributes which shall be made mandatory as mentioned below:

- a. Name
- b. Address
- c. PAN
- d. Valid mobile number
- e. Valid email-id
- f. Income range

⁵ Reference: CDSL/OPS/DP/P OLCY/4134 dated December 23, 2013

⁶ Reference: CDSL/OPS/DP/POLCY/2021/152 dated April 05, 2021



1.4.2 Checks for PAN

- a. The requirement of mandatory submission of PAN by clients for transactions in the securities market shall continue to apply, with permitted exemptions.
- b. DP shall verify the PAN online using the Income Tax site.
- c. In case PAN is not seeded with AADHAAR before the date specified by the Government, it will not be considered as a valid PAN.

1.4.3 Checks for mobile number and email ID

- a. DPs shall ensure that separate mobile number and email address is captured for all Beneficial Owner [BO] account holders. However, after submitting a written declaration, BO can update mobile number and email address of its family members. Family for this purpose has been defined as self, spouse, dependent parents and dependent children.
- b. In cases, wherein same mobile number / email ID is captured in more than 1 demat account and family flag is also not updated, DP shall be required to send 15 days notice to such demat account holder for submitting the mobile number /email ID Modification form /request letter for updating the same or family flag declaration, failure to comply with which would result in classification of such accounts as non-complaint accounts.
- c. DPs shall ensure that the mobile numbers/ email addresses of DPs /their KMPs/ other employees etc. are not captured.
- d. In case DP has the mobile number and email ID of the client in its back office, or trading account or in the bank account provided by the client and account is KYC complied in such trading account / bank account, the DP may update the details in the demat account and intimate the client about the updation by sending the Client Master Report [CMR] along with an intimation to complete the validation process.
- e. Following cannot be considered as valid mobile number:
 - 1. In respect of mobile numbers for India, Mobile no. is of 10 digit but starts with any number between 1 to 5 i.e. (1,2,3,4 & 5)
 - 2. '0000000000' / '1234567890' is captured.
 - 3. Single number is appearing in all 10 digit such as '1111111111', '2222222222', '3333333333', '4444444444', '5555555555', '6666666666', '7777777777', '8888888888', '9999999999'.
- f. Following cannot be considered as valid email ID:
 - 1. 'Noemail' is mentioned in email ID.
 - 2. '@' is not mentioned in email ID.
 - 3. If words - 'notprovided' and 'xyz' are mentioned in email id field.



4. Invalid email domain is mentioned. E.g. number digits are mentioned prior to domain name viz. 202Ggmail.com, 1234gmail.com, 1rediffmail.com, 55yahoo.com etc.
5. There is '.' (dot) at the end of Email ID
6. There is no '.' (dot) after '@' and before text
7. More than one '@' are there in email ID.

1.4.4 Income Range

- a. As per Additional Account opening, income range per annum is required to be obtained from clients.
 - b. The income range as required are as given below:
 - i. Income Range-Individuals
 - Below Rs. 1 lac
 - Rs. 1 lac to Rs. 5 lacs
 - Rs. 5 lacs to Rs. 10 lacs
 - Rs. 10 lacs to Rs. 25 lacs
 - More than Rs. 25 lacs
 - ii. Income Range-Non-Individuals
 - Below Rs. 1 lac
 - Rs. 1 lac to Rs. 5 lacs
 - Rs. 5 lacs to Rs. 10 lacs
 - Rs. 10 lacs to Rs. 25 lacs
 - Rs. 25 lacs to Rs. 1 crore
 - More than Rs. 1 crore
- 1.4.5 All 6-KYC attributes shall be mandatory for new accounts opened from August 1, 2021. In respect of all existing accounts, DPs must verify that all 6-KYC attributes are updated and wherever required necessary communication to be sent to their clients to update the same on or before June 30, 2022. DPs shall be required to inform the clients through both physical and electronic modes and also through its website, if any, for updating the details and complete the validation process. Thereafter, such non-compliant demat accounts will be liable to be made inactive i.e., no debit will be allowed in such demat account (except for settlement of already open positions).
- 1.4.6 Further, SEBI has also advised the depositories to instruct their DPs to ensure adequate due diligence while on-boarding of clients and conducting of KYC.



1.4.7 For the demat accounts of Institutional & non-Institutional clients / investors operated through custodians, Mandatory KYC attributes to be captured are:

	Institutional clients / investors		Non-institutional clients / investors	
	Details of Client	Details of Client's Custodian	Details of Client	Details of Client's Custodian (if applicable)
Name	Mandatory	Mandatory	Mandatory	Mandatory
PAN	Mandatory	Mandatory	Mandatory	Mandatory
Address	Mandatory	Mandatory	Mandatory	Mandatory
Valid Phone number	Mandatory (Mobile number OR Office Landline number)	Mandatory (Mobile number OR Office Landline number)	Mandatory (Mobile number)	Mandatory (Mobile number OR Office Landline number)
Valid Email-id	Mandatory	Mandatory	Mandatory	Mandatory
Income Range	Optional	-	Mandatory	-

- * An Institutional client / investor shall mean the categories of investors as per Section 1.1.12 of Chapter 4 of SEBI - MRD's Master Circular dated October 25, 2019.
- Foreign Institutional Investors registered with SEBI.
 - Mutual Funds registered with SEBI.
 - Public Financial Institutions as defined under section 4A of the Companies Act, 1956.
 - Banks i.e., a banking company as defined under Section 5(1)(c) of the Banking Regulations Act, 1949.
 - Insurance companies registered with IRDA.
 - Pension Fund regulated by Pension Fund Regulatory and Development Authority (PFRDA)
- Non-institutional client / investor would imply other than institutional client / investor.⁷

⁷ Reference: CDSL/OPS/DP/POLCY/2021/333 dated July 29, 2021



1.4.8 Email ID, Mobile Number or Landline Number and Income range shall be optional for category of client viz President of India, Central Government, State Government and the officials appointed by the courts e.g., Official liquidator, Court receiver etc. (under the category of Government).⁸

1.4.9 Income range shall be optional for category of client viz Bank – Depository Receipt (Banking entity which does not fall under definition defined u/s 5 (1) (c) of Banking Regulations Act, 1949 and such accounts held in relation to the Depository Receipts issued by Indian companies abroad).

1.5 Aadhaar seeding (Linkage of Aadhaar with PAN)⁹

1.5.1 In case PAN is not seeded with AADHAAR before the date specified by the Government; it will not be considered as a valid PAN.

1.5.2 After the timeline specified for PAN-Aadhaar linkage, the non-compliant demat accounts for linking of PAN and Aadhaar will be frozen for debit and credit.

1.6 Nomination

In addition to the procedure already specified in the Operating Instructions and the Bye Laws, the following additional guidelines with respect to Nomination shall require to be complied with:

1.6.1 Section 73 of Companies Act, 2013 provides for nomination by a holder of securities.¹⁰

1.6.2 Investors opening new demat account(s), shall have the choice of providing nomination or opting out nomination, as follows;

a. Nomination form

b. Opt out of nomination through 'Declaration Form'

1.6.3 In this regard, DPs shall activate new Demat accounts, only upon receipt of above formats.

⁸ Reference: CDSL/OPS/DP/POLCY/2021/595 dated December 28, 2021 and CDSL/OPS/DP/POLCY/2022/275 dated May 19, 2022

⁹ Reference: CDSL/OPS/DP/POLCY/2021/152 dated April 05, 2021

¹⁰ Reference: CDSL/OPS/DP/POLCY/2021/325 dated July 26, 2021



1.6.4 All existing eligible demat account holder/s shall provide choice of nomination as per the option given in paragraph 2 of SEBI circular dated July 23, 2021, on or before timelines prescribed, falling which the demat account shall be frozen for debits.

1.6.5 DP shall ensure that adequate systems are in place including for providing for eSign facility for online nomination facility and also take all necessary steps to maintain confidentiality and safety of client records.

1.6.6 The details required in the nomination form viz. mobile number, e-mail ID and identification details of the nominee(s)/ guardian(s) of the minor nominee(s) have been made optional.¹¹

1.7 Landmark details in the address:

1.7.1 If BO has added landmark details in the address column of the Account Opening / Letter, then DP can capture the same is CDAS, even though the same is not appearing in the proof of address documents, preceded by words such as:¹²

- above
- adjacent to
- behind
- near
- next to
- off
- opposite

1.8 Investor Charter¹³

1.8.1 DP should provide a copy of Investor Charter as a part of account opening kit to the clients, through email/ letters etc.

1.9 Account Opening by visually challenged persons

1.9.1 DPs are advised to ensure that all facilities including online facilities are offered to visually challenged persons without any discrimination and all possible assistance is provided to visually challenged persons for opening and operating demat accounts. DPs

¹¹ Reference: CDSL/OPS/DP/POLCY/2022/107 dated February 25, 2022

¹² Reference: CDSL/OPS/DP/POLCY/2516 dated June 24, 2011

¹³ Reference: CDSL/OPS/DP/POLCY/2021/589 dated December 25, 2021



should accordingly note that there are no special restrictions for visually challenged person for opening and operating a demat account subject to compliance with requirements as applicable to any other investor.¹⁴

1.10 HUF

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to HUF demat accounts shall require to be complied with:

In the event of death of Karta of HUF, the name of the deceased Karta in the Beneficial Owner (BO) account shall be replaced by the new Karta of the HUF who in such a case shall be eldest coparcener in the HUF or a coparcener who is appointed as Karta by an agreement reached amongst all the coparceners of the HUF.¹⁵

1.11 Opening of Basic Services Demat Account (BSDA)¹⁶

1.11.1 All DPs shall make available a "Basic Services Demat Account" (BSDA) with limited services as per terms specified.

1.11.2 Eligibility: Individuals shall be eligible to opt for BSDA subject to the following conditions-

- i. All the individuals who have or propose to have only one demat account where they are the sole or first holder.
- ii. Individuals having any other demat account/s where they are not the first holder shall be eligible for BSDA in respect of the single demat account where they are sole or first holder.
- iii. The individual shall have only one BSDA in his/her name across all depositories.
- iv. Value of holdings of debt securities held in the demat account shall not exceed Rupees Two Lakhs and value of holdings of other than debt securities held in the demat account shall not exceed Rupees Two Lakhs at any point of time.

¹⁴ Reference: CDSL/OPS/DP/POLCY/5202 dated May 19, 2015

¹⁵ Reference: CDSL/OPS/DP/POLCY/2022/496 dated August 29, 2022

¹⁶ Reference: CDSL/OPS/DP/P OLCY/3190 dated August 28, 2012



1.11.3 Option to open BSDA: The DP shall give option:

- i. To open BSDA to all eligible individuals who open a demat account after the date of applicability of this circular;
- ii. To all the existing eligible individuals to convert their demat account into BSDA on the date of the next billing cycle based on value of holding of securities in the account as on the last day of previous billing cycle.
- iii. To continue to reassess the eligibility of the individuals at the end of every billing cycle and give option to the individuals who are eligible to opt for BSDA.

1.11.4 Charges:

- i. The charge structure may be on a slab basis as indicated below
 - a. No Annual Maintenance Charges (AMC) shall be levied if the value of holdings of debt securities is up to Rs. 1 lakh and a maximum AMC of Rs. 100 shall be levied if the value of holdings of debt securities is between Rs. 1,00,001 and Rs.2,00,000.
And
 - b. No AMC shall be levied if the value of holdings other than debt securities is below Rs. 50,000 and a maximum AMC of Rs. 100 shall be levied if the value of holdings other than debt securities is between Rs.50,001 and Rs.2,00,000.¹⁷
- ii. The value of holding shall be determined by the DPs on the basis of the daily closing price or NAV of the securities or units of mutual funds, as the case may be. Where such price is not available the last traded price may be taken into account and for unlisted securities other than units of mutual funds, face value may be taken in to account. The value of suspended securities may not be considered for the purpose of determining eligibility of demat account as BSDA.
- iii. If the value of holding in such BSDA exceeds the prescribed criteria at any date, the DPs may levy charges as applicable to regular accounts (non BSDA) from that date onwards.
- iv. DPs shall assess the eligibility of the BOs at the end of the current billing cycle and convert eligible demat accounts into BSDA.

1.11.5 All BOs opting for the facility of BSDA, shall register their mobile number for availing the SMS alert facility for debit transactions.

¹⁷ Reference: CDSL/OPS/DP/POLCY/2019/200 dated April 18, 2019



1.11.6 At least Two Delivery Instruction Slips (DIS) shall be issued at the time of account opening.

1.11.7 Statements:

i. Transaction Statements:

- a. Transaction statements shall be sent to the BO at the end of each quarter. If there are no transactions in any quarter, no transaction statement may be sent for that quarter.
- b. If there are no transactions and no security balance in an account, then no further transaction statement needs to be provided.
- c. Transaction statement shall be required to be provided for the quarter in which the account became a zero balance account.

ii. Holding Statement:

- a. DP shall send atleast one annual physical statement of holding to the stated address of the BO in respect of accounts with no transaction and nil balance even after the account has remained in such state for one year. The DP shall inform the BO that the dispatch of the physical statement may be discontinued if the account continues to remain zero balance even after one year.
- b. One annual statement of holding shall be sent in respect of remaining accounts in physical or electronic form as opted for by the BO.

iii. Charges for statements: Electronic statements shall be provided free of cost. In case of physical statements, the DP shall provide at least two statements free of cost during the billing cycle. Additional physical statement may be charged at a fee not exceeding Rs.25/- per statement.

1.11.8 All other conditions as applicable to regular demat accounts, other than the ones mentioned in this circular shall continue to apply to basic services demat account.

1.12 SARAL Account Opening Form for resident individuals

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to SARAL Account Opening shall require to be complied with:



- 1.12.1 This form will be separately available with the DPs and can also be downloaded from the CDSL website.¹⁸
- 1.12.2 The Rights and Obligations of the Beneficial Owners and Depository Participant and documentary proof related to identity and address as specified in SEBI shall continue to remain applicable. It is further clarified that the provisions laid down under the PMLA shall also continue to remain applicable.
- 1.12.3 For these set of individual investors, it has been decided to simplify the requirement of submission of ‘proof of address’. Henceforth, individual investor may submit only one documentary proof of address (either residence/correspondence or permanent) while opening a demat account or while undergoing updation.
- 1.12.4 In case the proof of address furnished by the said investor is not the address where the investor is currently residing, the DP may take a declaration of the residence/correspondence address on which all correspondence will be made by the DP with the investor. 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, investor may intimate the new address for correspondence to the DP within two weeks of such a change. The residence/ correspondence address and any such change thereof may be verified by the DP through ‘positive confirmation’ such as (i) acknowledgment of receipt Welcome Kit/ dispatch of any periodical statement, etc. (ii) telephonic conversation; (iii) visits, etc.

1.13 Information to KYC Registration Agency (KRA)

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to KYC Registration Agency (KRA) shall require to be complied with:

- 1.13.1 It shall be mandatory for DPs to carry out IPV of their clients. The DP 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. The IPV carried out by other SEBI registered intermediary can be relied upon by DP. DPs are advised to note that persons who can carry out IPV may also carry out verification of documents with the originals.¹⁹

¹⁸ Reference: CDSL/OPS/DP/POLCY/5088 dated March 25, 2015 and CDSL/OPS/DP/POLCY/5311 dated July 13, 2015

¹⁹ Reference: CDSL/OPS/DP/POLCY/2774 dated December 27, 2011 and CDSL/A,I&C/DP/ POLCY/2806 dated January 12, 2012



- 1.13.2 Pursuant to amendments made in the SEBI {KYC Registration Agency (KRA)} Regulations, 2011, KRAs shall independently validate records of those clients (existing as well as new) whose KYC has been completed using Aadhaar as an OVD. The records of those clients whose have completed KYC using non-Aadhaar OVD shall be validated only upon receiving the Aadhaar Number.²⁰
- 1.13.3 KRAs shall promptly inform the respective DPs of deficiency/inadequacy in client's KYC documents, if any, that is observed for validation.
- 1.13.4 On successful completion of KYC validation, a unique client identifier called KRA identifier shall be assigned by KRA to the client and such KRA identifier may be used by the client for opening of account with any other intermediary, without repeating the KYC process.
- 1.13.5 The KYC records of new clients (who have used Aadhaar as an OVD) shall be validated within 2 days of receipt of KYC records by KRAs.
- 1.13.6 Clients whose KYC records are not found to be valid by KRA after the validation process shall be allowed to transact in securities market only after their KYC is validated.
- 1.13.7 In case of KYC based on non-Aadhaar OVD, the KRA shall only store such records and the same would not be validated by KRAs unless Aadhaar number is provided by the client.
- 1.13.8 SEBI vide their email dated March 31, 2023 has informed that certain demat accounts have been created/opened with the Depository by the DPs for certain PANs, for which KYC validation has been declared non valid by KRAs. The clients whose KYC records are not found to be valid by KRA after the validation process, shall not be allowed to transact in securities market.²¹

1.14 Operationalisation of Central KYC records Registry (CKYCR)²²

- 1.14.1 As per the 2015 amendment to PML (Maintenance of Records) Rules, 2005 (the rules), the DP being reporting entity shall capture the KYC information for sharing with the Central KYC Records Registry in the manner mentioned in the Rules, as per the KYC templates finalised by CERSAI.

²⁰ Reference: CDSL/OPS/DP/P OLCY/2022/202 dated April 08, 2022

²¹ Reference: CDSL/OPS/DP/P OLCY/2023/207 dated March 31, 2023

²² Reference: CDSL/OPS/DP/POLCY/6244 dated November 11, 2016 and CDSL/OPS/DP/POLCY/6049 dated July 29, 2016



1.14.2 DPs are advised to upload and register the records of individual clients and legal entities on CKYCR.²³

1.14.3 This is not applicable to FPIs.

1.14.4 DPs are advised to refer SEBI circular no. CIR/MIRSD/120/2016 Dated November 10, 2016 regarding Uploading of the existing clients' KYC details with CKYCR System.

1.15 Aadhaar based e-KYC process

1.15.1 SEBI has clarified that in consultation with UIDAI and the market participants, it was decided to accept e-KYC service launched by UIDAI also, as a valid process for KYC verification. The information containing relevant client details and photograph made available from UIDAI as a result of e-KYC process shall be treated as sufficient Proof of identity and Address of the client.²⁴

1.15.2 It is also clarified that the usage of Aadhaar card as issued by the UIDAI is voluntary.²⁵

1.15.3 DP, 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.

1.15.4 Upon notification by the Central Government / registration with UIDAI, the KUAs and sub-KUAs shall adopt the following process for Aadhaar e-KYC of investors (resident) in the securities market and as may be prescribed by UIDAI from time to time.

1.15.5 Online Portal based Investor (Resident) e-KYC Process (Aadhaar as an OVD)

- a. Investor visits portal of KUA Sub-KUA to open account/invest through intermediary.
- b. For Aadhaar e-KYC, investor is redirected to KUA portal. Investor 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.
- c. Investor will receive OTP in mobile number registered with Aadhaar. Investor enters the OTP sent by UIDAI on KUA portal for Aadhaar e-KYC.

²³ Reference: CDSL/OPS/DP/POLCY/2021/122 dated March 18, 2021

²⁴ Reference: CDSL/OPS/DP/POLCY/3969 dated October 09, 2013

²⁵ Reference: CDSL/OPS/DP/POLCY/2019/560 dated November 06, 2019



- d. KUA will receive the e-KYC details from UIDAI upon successful Aadhaar authentication which will be further forwarded to Sub-KUA in encrypted format (using KUAs own encryption key) and will be displayed to the investor on portal. Sharing of e-KYC data by the KUA with Sub-KUA may be allowed under Regulation 16(2) of Aadhaar (Authentication) Regulation, 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 investor consent.
- e. Investor will fill the additional detail as required under KYC format.
- f. Sub-KUA will upload additional KYC details to the KUA.

1.15.6 Assisted Investor (Resident) e-KYC process (Aadhaar as an OVD)

- i. Investor approaches any of the Sub-KUAs for e-KYC through Aadhaar.
- ii. Sub-KUAs will perform e-KYC using registered / Whitelisted devices with KUAs.
- iii. KUA will ensure that all devices and device operators of Sub-KUA are registered / whitelisted devices with KUA.
- iv. Investor will enter Aadhaar No. or Virtual Id and provides consent on the registered device.
- v. Investor provides biometric on the registered device.
- vi. Sub-KUA fetches the e-KYC details through the KUA from UIDAI which will be displayed to the investor on the registered device.
- vii. Investor will also provide the additional detail as required.

1.15.7 The KUA/ sub-KUA while performing the Aadhaar authentication shall also comply with the following:

- a. 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.
- b. 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.
- c. e-KYC data received as response upon successful Aadhaar authentication from UIDAI will be stored by KUA and Sub-KUA in the manner prescribed by Aadhaar Act/Regulations and circulars issued by UIDAI time to time.
- d. 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).



- e. 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.
- f. 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.
- g. 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.
- h. 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.
- i. Monitoring of irregular transactions - KUAs shall develop appropriate monitoring mechanism to record irregular transactions and their reporting to UIDAI.
- j. Investor Grievance Handling Mechanism - Investor may approach KUA for their grievance redressal. KUA will ensure that the grievance is redressed within the timeframe as prescribed by UIDAI. KUA will also submit report on grievance redressal to UIDAI as per timelines prescribed by UIDAI.

1.15.8 Onboarding process of KUA/Sub-KUA by UIDAI:

- a. 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.
- b. For appointment of DP as Sub-KUAs, KUA will send list of proposed Sub-KUAs to SEBI and SEBI would forward the list of recommended Sub-KUAs to UIDAI for onboarding. An agreement will be signed between KUA and Sub-KUA, as prescribed by UIDAI. Sub-KUA shall also comply with the Aadhaar Act Regulations, circulars, Guidelines etc. issued by UIDAI from time to time.
- c. Each sub-KUA shall be assigned a separate Sub-KUA code by UIDAI.

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

1.15.10 For non-compliances if any observed on the part of the reporting entities (KUAs/ Sub-KUAs), SEBI may take necessary action under the applicable laws and also bring the same to the notice of DoR / FIU for further necessary action, if any. Reporting entity (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. Based on a report from SEBI / UIDAI or otherwise, if it is found that the reporting entity no longer fulfills 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.

1.16 Online KYC Process and Use of Technology for KYC²⁶

1.16.1 In case a Depository Participant is doing online KYC, it shall comply with the following guidelines prescribed by SEBI/CDSL:

- a) A DP shall obtain the express consent of the investor before undertaking online KYC.
- b) In order to enable the online KYC process for establishing account based relationship with the DP, Investor's KYC can be completed through online /App based KYC, in-person verification through video, online submission of Officially Valid Document (OVD) / other documents under eSign.
- c) The investor shall visit the website/App/digital platform of the DP and fills up the online KYC form and submits requisite documents online.
- d) The name, photograph, address, mobile number, email ID, Bank details of the investor shall be captured online and OVD / PAN / signed cancelled cheque shall be provided as a photo / scan of the original under eSign.
- e) A DP shall verify Mobile and email through One Time Password (OTP) or other verifiable mechanism. The mobile number/s of investor accepted as part of KYC should preferably be the one seeded with Aadhaar. A DP shall ensure to meet the requirements of the mobile number and email as detailed under Communique No. CDSL/OPS/DP/POLCY/5139 dated April 15, 2015.
- f) Aadhaar shall be verified through UIDAI's authentication / verification mechanism. In case the investor submits his/her Aadhaar number, a DP shall ensure that such investor to redact or blackout his/her Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under PML Rule 9 (15). A DP shall not store/ save the Aadhaar number of investor in its system. e-KYC through Aadhaar Authentication service of UIDAI or offline verification through Aadhaar QR Code/ XML file can be undertaken, provided the XML file or Aadhaar

²⁶ Reference: CDSL/OPS/DP/POLCY/2020/203 dated April 27, 2020



Secure QR Code generation date is not older than 3 days from the date of carrying out KYC. A DP shall ensure that the usage of Aadhaar is optional and purely on a voluntary basis by the investor.

- g) PAN shall be verified online using the Income Tax Database.
- h) Bank account details shall be verified by Penny Drop mechanism or any other mechanism using API of the Bank. Based on bank details in the copy of the cancelled cheque provided by the investor, the money is deposited into the bank account of the investors to fetch the bank account details and name.) The name and bank details as obtained shall be verified with the information provided by investor.
- i) Any OVD other than Aadhaar shall be submitted through Digiocker / under eSign mechanism.
- j) In terms of Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules) “Officially Valid Documents” means the following:
 - a. the passport,
 - b. the driving licence,
 - c. proof of possession of Aadhaar number,
 - d. the Voter's Identity Card issued by Election Commission of India,
 - e. job card issued by NREGA duly signed by an officer of the State Government and
 - f. the letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the Regulator.
- k) Further, Rule 9(18) of PML Rules states that in case OVD furnished by the investor does not contain updated address, the document as prescribed therein in the above stated Rule shall be deemed to be the OVD for the limited purpose of proof of address.
- l) PML Rules allows an investor to submit other OVD instead of PAN, however, in terms of SEBI circular No. MRD/DoP/Cir- 05/2007 dated April 27, 2007 the requirement of mandatory submission of PAN by the investors for transaction in the securities market shall continue to apply.



- m) Once all the information as required as per the online KYC form is filled up by the investor, KYC process could be completed as under:
 - i. The investor would 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 DP under eSign, or
 - ii. Affix online the cropped signature on the filled KYC form and submit the same to the DP under eSign.
 - n) The DP shall forward the KYC completion intimation letter through registered post/ speed post or courier, to the address of the investor in cases where the investor has given address other than as given in the OVD. 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 CDSL.
 - o) The original seen and verified requirement for OVD would be met where the investor provides the OVD in the following manner:
 - i. As a clear photograph or scanned copy of the original OVD, through the eSign mechanism, or;
 - ii. As digitally signed document of the OVD, issued to the DigiLocker by the issuing authority.
 - p) Further, IPV / VIPV shall not be required by the DP
 - i. when the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI.
 - ii. when the KYC form has been submitted online, documents have been provided through digilocker or any other source which could be verified online.
- 1.16.2 **Features for online KYC App of the DP** – DP may implement its own Application (App) for undertaking online KYC of investors. The App shall facilitate taking photograph, scanning, acceptance of OVD through Digilocker, video capturing in live environment, usage of the App only by authorized person of the DP. The App shall also have features of random action initiation for investor response to establish that the interactions not pre-recorded, time stamping, geo-location tagging to ensure physical location in India etc is also implemented. DP shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. DP shall carry out the liveness check in order to guard against spoofing and such other fraudulent manipulations. The DP shall before rolling out and periodically, carry out software and security audit and validation of their App. The DP may have additional safety and security features other than as prescribed above.



1.16.3 Feature for Video in Person Verification (VIPV) for Individuals – To enable ease of completing IPV of an investor, DP may undertake the VIPV of an individual investor through its App. The following process shall be adopted in this regard:

- i. DP through their authorised official, specifically trained for this purpose, may undertake live VIPV of an individual customer, 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.
- ii. The VIPV shall be in a live environment.
- iii. The VIPV shall be clear and still, the investor in the video shall be easily recognisable and shall not be covering their face in any manner.
- iv. The VIPV process shall include random question and response from the investor including displaying the OVD, KYC form and signature or could also be confirmed by an OTP.
- v. The DP shall ensure that photograph of the customer downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV.
- vi. The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.
- vii. The DP may have additional safety and security features other than as prescribed above.

1.16.4 FAQs on online KYC process and use of technology²⁷

- a) There is no requirement to verify the OVD/other documents in case of receipt of photograph or scan copy of the original OVD with e-sign of the client. Self-attestation by the client through the esign will be considered as sufficient and will satisfy the requirement of verification by DP. DP can verify the details provided by the client matches with the details on the OVD/other documents.
- b) It is mandatory to take live photograph of the client in all cases of online account opening through the website/App/digital platform of the DP, whether the account is opened through the Aadhaar as OVD, any other OVD or through download of KYC from KRA. It is not permitted to upload the photograph of the client or take of photograph of the client photograph. Online KYC App of the DP should verify the liveliness of the photograph.

²⁷ Reference: CDSL/OPS/DP/POLCY/2020/444 dated October 14, 2020



- c) Signature of the client can be cropped from a signed cancelled cheque, signature on a white paper or signature made on the screen of a device, provided such cropped signature on the document / screen is eSigned by the client and submitted to the DP. However, before esigning the document, the cropped signature should be inserted in the place holders of the KYC form and displayed to the investor.
- d) DP shall verify the e-sign of the client on the basis of name, gender and year of birth mentioned in the e-sign certificate and comparing the same with the client details available in its record.
- e) As per the procedure mentioned in the IT Act 2000, digital signature on the electronic document can be verified using the public key of the signature.
- f) If KYC is conducted based on Aadhaar Authentication, IPV/VIPV would not be required, however, DPs should perform minimum due diligence to ensure authenticity of the data provided. Accordingly, IPV/VIPV is not required in following cases:
 - i. OTP based e-KYC
 - ii. Biometric based e-KYC
 - iii. Offline verification of XML file
 - iv. Offline verification of Aadhaar QR Code
 - v. OVD's downloaded from Digilocker
 - vi. KYC downloaded from KRA and client consent by OTP
 - vii. Documents from any other source which could be verified online.IPV/VIPV will be required in case when the investor submits scanned copies of any OVD as prescribed by SEBI.
- g) PAN is not included under the list of OVD's under the rule 2(d) of the PML rules. Hence, it can't be considered as a proof of identity however, it is mandatory to provide copy of PAN card. A photograph/scan of PAN should be provided by client under his e-sign or e-PAN can be provided through Digilocker which are issued directly by issuing authority to Digilocker.
- h) The scan of the OVD means that original OVD is scanned using the scanning software or through the physical scanner available. It doesn't include the photocopy of the original document.



- i) In cases where client is identified by using e-KYC through Aadhaar authentication services of UIDAI or offline verification through Aadhaar QR code/XML file , the client shall provide mobile number as updated in their Aadhaar. Where KYC is done by relying upon OVD other than Aadhaar, in such case, the mobile number/s of investor accepted as part of KYC should preferably be the one seeded with Aadhaar. The Mobile number will be verified by DP through One Time Password (OTP) or other verifiable mechanism.
- j) It is mandatory to submit email id at the time of account opening using online account facility. DP shall verify the email-id using OTP / other verifiable mechanism.
- k) A scanned image or photo of OVD submitted by the client to the RI through video IPV or other online mechanisms cannot be considered as a valid proof. The OVD shown in the VIPV should have been validated by means of an electronic copy issued in the Digilocker under the valid signature of the issuing authority. Hence, any documents being obtained from the client outside this mechanism should be mandatorily obtained as a scanned image or photo under eSign.
- l) If DP is availing penny drop facility using API of the bank, copy of signed cancelled cheque is not required to be obtained from client. However, in cases where penny drop match fails, or in cases where penny drop doesn't return joint account holder name, clients should be asked to submit proofs like copy of signed cancelled cheque,
- m) The DP shall attempt verification of bank account details using penny drop facility in all cases. But, if the investor's bank does not provide response to support the penny drop facility, the bank details can be accepted based on the copy of the signed cancelled cheque.
- n) If the OVD furnished by the client does not contain the updated address, the documents such as. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill) OR Property etc, will be treated as deemed OVD 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 above documents. In case of non-receipt of the updated OVDs, no transactions shall be allowed in such account and intimation shall also sent to the CDSL.



- o) In cases where the investor has given address other than as given in the OVD and the KYC completion documents sent to the clients have been returned undelivered, the account should be frozen for further transactions and the intimation should accordingly be sent to the client on mobile number and email id or on the permanent address of the client.
 - p) A digitally signed Aadhar, issued to the DigiLocker by UIDAI can be accepted as an OVD under eSign of the client.
 - q) The online KYC application of DP should have a facility to take a photograph of the investor which has time stamping, geo-location tagging and liveness check.
- 1.16.5 DPs are requested to take note that where the DP is opening an account online based on download of KYC details from the KRA, the KYC details as downloaded from the KRA shall be displayed to the client at the time of account opening where the client must confirm that there is no change in the particulars as downloaded from KRA and in case of any change, the client must be provided an option to provide latest details along with supporting documentation.²⁸
- 1.16.6 Online demat account opening shall be allowed in addition to Sole resident individual and Joint holders, for other individual and non-individual accounts also. The accounts may not be opened online in the strict sense of processing of account opening but would be more like a semi-automated system, as the documents submitted electronically or otherwise would be checked by the DP. DPs should ensure that the documents obtained are as per the CDSL bye laws and Operating Instructions and then put into the CDSL system for account opening. Further, the account opening forms and the supporting documents; if any, will be e-signed / digitally signed by the holder / concerned authorized persons.²⁹
- 1.16.7 New demat accounts can be opened in the online mode for the following client types also.
- 1. Non-Resident Indian with repatriation (NRE)
 - 2. Non-Resident Indian without repatriation (NRO)
 - 3. Guardian on behalf of the Minor account holder
 - 4. Corporate Account
 - 5. HUF Account

²⁸ Reference: CDSL/OPS/DP/ POLCY/2021/127 dated March 22, 2021

²⁹ Reference: CDSL/OPS/DP/GENRL/2021/447 dated October 04, 2021 and CDSL/OPS/DP/GENRL/2021/518 dated November 17, 2021



6. Registered Trust
7. Registered Society
8. Bank
9. Mutual Fund
10. Partnership Firm through the partners
11. Unregistered trust through the trustees
12. Unregistered societies through the trustees

1.16.8 The following checks and balances are required to be taken care by the DPs for online account opening:

- a. The investor is required to use Aadhaar for online account opening.
- b. The documents viz. proof of identity, account opening form copy of cheque, etc. needs to signed electronically using the Aadhaar (e-signed).
- c. The email ID is validated.
- d. The mobile number is validated.

DPs are advised to take note of the same and ensure compliance for opening of online demat account.

1.16.9 It is reiterated that all the requirements and processes laid down by SEBI needs to be followed while opening any demat account/s through online mode.

1.16.10 It is clarified that any document, except for the documents mentioned in the First Schedule of the IT Act 2000, may be authenticated by an investor by way of electronic/digital signature including Aadhaar eSign. Therefore, the process of performing KYC can be completed by using electronic/digital signature including Aadhaar eSign. In case of non-individual clients, DPs may take caution and satisfy themselves regarding the genuineness of the authorization and identity of the authorized signatories.

1.16.11 With regard to requirement of geo-tagging in India, it is reiterated that while completing the investor's KYC through KYC app of DP, the DP shall continue to ensure the requirement of geo-tagging with the investor's physical location in India as per SEBI guidelines till further clarification is issued in the matter.³⁰

³⁰ Reference: CDSL/OPS/DP/POLCY/2022/67 dated February 07, 2022



1.17 Guidelines on Identification of Beneficial Ownership³¹

1.17.1 The DPs shall comply with the following guidelines in respect of identification of Beneficial Ownership.

1.17.2 **For clients other than individuals or trusts:** Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the DP shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

- a) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest;

Explanation: Controlling ownership interest means owner-ship of/ entitlement to:

- i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
- ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

- b) In cases where there exists doubt under clause (a) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means;

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

- c) Where no natural person is identified under clauses (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

1.17.3 **For client which is a trust:** Where the client is a trust, the DP shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the author of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership;

³¹ Reference: CDSL/OPS/DP/POLCY/3451 dated January 25, 2013



1.17.4 Exemption in case of listed companies: Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies;

1.17.5 Applicability for foreign investors: DP dealing with foreign investors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client.

1.18 Mapping of Unique Client Code with Demat Accounts³²

1.18.1 DPs are required to obtain UCC along with corresponding exchange ID at the time of demat account opening or with Modification from their clients.³³

1.18.2 Provision is made in the Demat Account Opening form to mention the UCC details of the sole / first holder of Demat Account.

1.18.3 UCC allotted by the trading member (TM) to the client shall be mapped with the demat account of the client.

1.18.4 A client may trade through multiple TMs in which case each such UCC shall be mapped with one or more demat account(s).

1.18.5 DPs are advised to incorporate necessary changes in their back-office software, if any.

1.18.6 DPs are once again advised to inform their Clearing Member (CM), Trading Member (TM) and Trading Clients to take utmost care for correctness of UCC details while providing the said details to DPs.

1.18.7 Further, DPs too are required to take due precautions while capturing the said details in CDSL system so that UCC details being correctly mapped with the demat account.

³² Reference: CDSL/OPS/DP/POLCY/2019/580 dated November 18, 2019

³³ Reference: CDSL/OPS/DP/POLCY/2020/141 dated March 16, 2020



1.18.8 DPs are hereby directed to disseminate the aforesaid guidelines to their CM / TM / Trading clients to help them to understand and comply with the guidelines in accordance with the SEBI guidelines so that failure of pay-in transaction, if any, on account of non-mapping of UCC details with the demat account of clients due to incorrect UCC – PAN details captured in demat account vis-à-vis corresponding details received from the Stock Exchange(s) can be avoided.³⁴

1.19 Power Of Attorney (POA) / Demat Debit and Pledge Instruction (DDPI)

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to POA/DDPI shall require to be complied with:

1.19.1 A BO may execute the DDPI for the following purpose:³⁵

- a) Transfer of securities held in the beneficial owner accounts of the client towards Stock Exchange related deliveries / settlement obligations arising out of trades executed by clients on the Stock Exchange through the same stock broker
- b) Pledging / re-pledging of securities in favour of trading member (TM) / clearing member (CM) for the purpose of meeting margin requirements of the clients in connection with the trades executed by the clients on the Stock Exchange.
- c) Mutual Fund transactions being executed on stock exchange order entry platforms and which shall be in compliance with SEBI circulars SEBI/HO/IMD/IMD-I DOF5/P/CIR/2021/634 dated October 04, 2021, SEBI/HO/IMD/IMD-I DOF5/P/CIR/2021/635 dated October 04, 2021 and SEBI/HO/IMD/IMD-I DOF5/P/CIR/2022/29 dated March 15, 2022 or any other circular which may be issued in this regard; and
- d) Tendering shares in open offers which shall be in compliance with SEBI circular SEBI/HO/CFD/DCR-III/CIR/P/2021/615 dated August 13, 2021 or any other circular which may be issued in this regard.

³⁴ Reference: CDSL/OPS/DP/S ETTL/2023/65 dated January 31, 2023

³⁵ Reference: CDSL/OPS/DP/POLCY/2022/194 April 05, 2022 and CDSL/OPS/DP/P OLCY/2022/585 October 7, 2022



1.20 Portfolio Management Services (PMS) Power of Attorney (POA)³⁶

1.20.1 PMS managers have to open the new PMS POA account to be linked only to the PMS client accounts.

1.20.2 SEBI Registration Number of the PMS Manager is mandatory for PMS POA.

1.20.3 The Custodian CM accounts has to be mapped to the new PMS POA.

1.21 Opening of Margin Pledge & Repledge account³⁷

1.21.1 To enable clients to pledge their securities as collateral / margin to a TM / CM, DP shall open accounts titled 'TM – Client Securities Margin Pledge Account (TM-CMPA)' and 'CM – Client Securities Margin Pledge Account (CM-CMPA)' with new types / sub-types.

1.21.2 In case a TM/CM's existing pool account is maintained with a DP and the TM-CMPA / CM-CMPA / TM/CM-CMPA is being opened with the same DP then fresh Account Opening Form (AOF) would not be required to be submitted by a TM / CM to the DP. DP shall obtain a consent from a TM / CM in the prescribed format along with a copy of the board resolution for the same. However, if the TM-CMPA / CM-CMPA / TM/CM-CMPA is being opened with another DP where pool account is not maintained then the documents as applicable for opening of demat accounts mentioned in the Operating Instructions would have to be furnished. ³⁸

1.21.3 A provision has been enabled to a member who is a TM and have appointed Professional Clearing Member (PCM) to settle transactions of all segments, can open 'TM – Client Securities Margin Pledge Account (TM-CMPA)'.³⁹

1.21.4 Similarly, if a member is a TM who is also a Self-Clearing Member (SCM) and settles transactions of all segments themselves can open 'CM – Client Securities Margin Pledge Account (CM-CMPA)'.

1.21.5 Also, if a member is only a PCM and settles transactions on behalf of the TMs can open 'CM – Client Securities Margin Pledge Account (CM-CMPA)'.

³⁶ Reference: CDSL/OPS/DP/SYSTM/2022/166 dated March 25, 2022

³⁷ Reference: CDSL/OPS/DP/P OLCY/2020/115 dated March 02, 2020

³⁸ Reference: CDSL/OPS/DP/POLCY/2020/234 dated May 22, 2020

³⁹ Reference: CDSL/OPS/DP/POLCY/2020/309 dated July 16, 2020



- 1.21.6 DPs shall open ‘TM/CM – Client Securities Margin Pledge Account (TM/CM-CMPA)’ for a member where if a TM has appointed PCM to settle its transactions in one/multiple segment/s and is a SCM in one/multiple segment/s to settle its own transactions.
- 1.21.7 CM / TM shall be required to close all their existing demat accounts tagged as ‘CM/TM Client Collateral Account’ and ‘CM/TM Collateral Account’.
- 1.21.8 DPs are directed to disseminate the aforesaid information / requirements / guidelines to their TM / CM clients to help them to understand and comply with the guidelines in accordance with the SEBI circular and ensure that the suitable back-office changes where applicable are implemented.

1.22 Opening of Client Securities Margin Funding Account⁴⁰

- 1.22.1 As directed by SEBI, funded stocks held by the TM / CM under the margin trading facility shall allowed to be held by the TM / CM only by way of pledge.
- 1.22.2 DP shall open an account of the new type ‘Client Securities Margin Funding Account’ (CMFA) so that securities purchased under margin trading facility i.e. funded stocks can be pledged by the client in this account.
- 1.22.3 In case a TM/CM’s existing pool account is maintained with a DP and the CMFA is being opened with the same DP then fresh Account Opening Form (AOF) would not be required to be submitted by a TM / CM to the DP for opening the CMFA. DP shall obtain a consent from a TM / CM in the prescribed format along with a copy of the board resolution for the same. However, if the CMFA is being opened with another DP where pool account is not maintained then the documents as applicable for opening of demat accounts mentioned in the Operating Instructions would have to be furnished. A TM / CM should mention the type of account as CMFA in the AOF.

1.23 Opening of Client Unpaid Securities Pledgee Account⁴¹

- 1.23.1 TM/CM will be required to maintain a new demat account viz. ‘Client Unpaid Securities Pledgee Account (CUSPA)’. DPs shall open CUSPA for their TM/CM clients with new BO-Status and BO-Sub-Status.

⁴⁰ Reference: CDSL/OPS/DP/POLCY/2020/309 dated July 16, 2020

⁴¹ Reference: CDSL/OPS/DP/POLCY/2022/658 dated November 11, 2022



- 1.23.2 While opening CUSPA, DPs are requested to take utmost care to ensure that PAN of CUSPA and corresponding settlement accounts of a TM/CM should be identical. Failing which transfer of pay-out securities from CM's Pool Account (TM/CM Pool Account as either TM/CM Principal Account – BSE TM/ICCL CM or TM/CM Pool Account – BSE TM/ICCL CM or Trading/Clearing Member Account – non-BSE/ICCL TM/CM) to demat account of unpaid client followed by auto pledge in corresponding CUSPA will be failed.
- 1.23.3 TM/CM may open Stock Exchange (SE) / Clearing Corporation (CC) wise CUSPA or alternatively may have a single CUSPA irrespective of CC / SE combination.
- 1.23.4 If TM/CM opts to open the CUSPA with a DP with whom the TM/CM has an existing TM/CM account, then a consent form as prescribed for the same may be obtained by DP from TM/CM. However, if TM/CM opts to open CUSPA with a DP with whom TM/CM does not have an existing TM/CM account, then TM/CM will be required to follow the account opening process as per the DP Operating Instructions.⁴²
- 1.23.5 All the active Client Unpaid Securities Account (CUSA), if any, are required to be 'closed'. Securities held in CUSA are either required to be disposed off / sold in the market or be transferred to the client's demat account by the TM/CM accordingly. CUSA which are not closed, will be frozen for both debit and credit.
- 1.23.6 DPs are directed to disseminate the aforesaid information / requirements / guidelines to their TM/CM/Trading clients to help them to understand and comply with the guidelines in accordance with the SEBI guidelines and ensure that the suitable back-office related changes where applicable are implemented.
- 1.23.7 DP shall open 'TM/CM – Client Unpaid Securities Pledge Account (TM/CM-CUSPA)' with new BO-Status and BO-Sub-Status, where a TM has appointed PCM to settle its transactions in one/multiple segment/s and is a SCM in one/multiple segment/s to settle its own transactions.⁴³

⁴² Reference: CDSL/OPS/DP/SETTL/2023/151 dated March 09, 2023

⁴³ Reference: CDSL/OPS/DP/SETTL/2023/178 dated March 21, 2023



1.24 Foreign Portfolio Investors

- 1.24.1 A foreign portfolio investor (FPI) shall make an application for the grant of certificate to a Designated Depository Participant ('DDP') in the Form and manner specified by the Government or the SEBI from time to time and shall be supported by the fee as specified and any documents in the manner specified by the SEBI from time to time.⁴⁴
- 1.24.2 FPIs are required to provide KYC related documents based on the category under which it is registered.
- 1.24.3 The DDP may grant FPI registration to the applicant on the basis of scanned copies of executed Common Application Form ('CAF'), scanned copies of certified supporting documents and applicable fees submitted by the applicant.
- 1.24.4 The DDP shall thereafter update the CAF module as per the standard process, for issuance of Permanent Account Number ('PAN').
- 1.24.5 Post allotment of PAN to the applicant, the scanned copies of certified Know Your Client ('KYC') documents of the applicant shall be uploaded on the KYC Registration Agencies ('KRA') by the DDP/ Custodian. Other intermediaries/ entities may access such documents from the KRA and complete their KYC requirements for opening the demat, trading and bank accounts.
- 1.24.6 Use of Digital Signatures by FPIs: FPIs may use digital signatures for the purpose of execution of CAF and other registration related documents, provided such digital signatures are in accordance with the provisions of the Information Technology Act, 2000.
- 1.24.7 The Custodian shall ensure that appropriate systems and procedures are in place to prevent any activity in such accounts till verification of physical documents is carried out.
- 1.24.8 Only upon receipt and verification of the physical documents by the DDP/ Custodian, the Custodian shall make an application to the Clearing Corporation ('CC') for allotment of a CP Code to the FPI and carry out necessary steps for enabling the FPI to transact in the Indian securities markets.

⁴⁴ Reference: CDSL/OPS/DP/POLCY/2023/204 dated March 31, 2023



1.24.9 Guidelines for KYC:⁴⁵

- i. Copies of all the documents submitted by the applicant should be accompanied by originals for verification. In case the original of any document is not produced for verification, then the copies should be properly attested by entities authorized for attesting the documents. Additional requirement of self-certification of documents is no longer required. In lieu of physical attestation, certification of copies of original documents by authorized bank officials (i.e. officials of Multinational Foreign Banks or any Bank regulated by RBI) through SWIFT mechanism may be accepted by DDPs/ Custodians for the purpose of verification of documents. The authorized bank official shall be required to send copies of original documents to the DDP/Custodian digitally and certify the authenticity of these documents through authentic free format SWIFT message types (such as SWIFT MT 599) sent to the DDP/ Custodian.
- ii. If any proof of identity or address is in a foreign language, then translation into English is required.
- iii. Name & address of the applicant mentioned on Form, should match with the documentary proof submitted.
- iv. If more than one address is provided, proof should be enclosed.
- v. The Global Custodian or the Local Custodian may fill the Form, if authorized through the Power of Attorney (PoA).
- vi. In person verification is not applicable for a non-individual Client. IPV for individual clients through web camera shall be allowed.
- vii. Reliance on information available from reliable public sources- In addition to information provided by the client, the intermediaries can rely on documents / information available from reliable public sources (for e.g. websites of Regulators, Exchanges, SROs, Registrars) while collecting documents / information required for an FPI. Attestation of these documents (by way of mentioning the source of the document and signature against the same) may be carried out by a duly authorized official of the Intermediary. No further attestation of such documents is required.
- viii. List of people authorized to attest the documents: Notary Public, officials of Multinational Foreign Banks or any Bank regulated by Reserve Bank of India (Name, Designation & Seal should be affixed on the copy).
- ix. The E-PAN issued by CBDT can also be produced by FPI for KYC compliance.

⁴⁵ Reference: CDSL/OPS/DP/POLCY/2022/733 dated December 29, 2022



- 1.24.10 Submission of unique investor group ID by FPI applicants in lieu of complete details of group constituents: FPI applicant, at the time of registration, is required to provide details of FPIs with whom it share ownership of more than fifty percent or common control, under the 'Clubbing of Investment Limit' section of the CAF. Depositories in turn generate a unique FPI investor group ID for identifying each such FPI investor group.
- 1.24.11 Apart from the KYC requirement stated below, each intermediary may have additional documentation requirement for conducting enhanced due diligence as per their internal policies.
- 1.24.12 In case, a FPI holds separate depository accounts in both NSDL and CDSL, it is allowed to appoint only one custodian.
- 1.24.13 DPs/DDPs are advised to refer SEBI Circular No. SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 regarding the 'Master Circular for Foreign Portfolio Investors, Designated Depository Participants and Eligible Foreign Investors' and SEBI Circular no. SEBI/HO/AFD/P/CIR/2023/043 dated March 27, 2023, regarding Streamlining the onboarding process of FPIs.

1.25 Constituents' Subsidiary General Ledger (CSGL) Account⁴⁶

- 1.25.1 DPs should comply with the guidelines issued by Reserve Bank of India vide notification no. 183 Dated September 05, 2011 and further amendment issued vide notification no. 135 Dated May 22, 2012 regarding conditions applicable for opening and maintenance of a Constituents' Subsidiary General Ledger (CSGL) account, as also the records to be maintained and procedures to be adopted by the CSGL account holders for safeguarding the interests of their constituents.

1.26 KYC Reconfirmation of Sikkim Based Demat Accounts⁴⁷

- 1.26.1 Process to be followed w.r.t. Newly onboarded Sikkim based demat accounts:
- 1.26.2 With respect to newly onboarded Sikkim based demat accounts; DPs will have to get all the demat accounts audited by their Auditor. In case of any adverse observations by the Auditors, DPs shall freeze the demat accounts of such clients and inform the client to rectify the discrepancy. Such demat account will be activated by DP only after KYC compliance by client and get it audited from Auditor. In case the discrepancies / error is on the part of DP, then it will have to be rectified by the DP at the earliest.

⁴⁶ Reference: CDSL/OPS/DP/POLCY/2671 dated October 05, 2011 and CDSL/OPS/DP/POLCY/3121 dated July 23, 2012

⁴⁷ Reference: CDSL/A,I&C/DP/POLCY/2022/458 dated August 11, 2022



Chapter 2 : Account Modification

2.1 Change in name

2.1.1 Updation of change in name of Beneficial Owner in case of Individual: ⁴⁸

- a) Investors residing in the State of Karnataka and Punjab, the name change is published by the State Government in the Official Gazette only for Government employees and not for private persons in case of change of name of an individual. Accordingly, it has been decided that in case of change of name of an individual in these states for reasons other than marriage, the same may be allowed for the individual in the BO account subject to the submission of following documents
 - i. Request letter for change of name,
 - ii. Sworn affidavit executed before the Notary Public/ Magistrate of First Class/ Executive Magistrate mentioning the reason for change of name and his complete address,
 - iii. Paper publication in one local newspaper and one national newspaper,
 - iv. KYC in changed name.
- b) DPs should obtain self-attested copies of above documents and verify with originals.

2.1.2 Minor correction in name of individual demat account holder⁴⁸

- a) DP shall ensure that the demat account holder whose name is to be corrected submits a duly filled and signed modification form or a request letter having all the details of the modification form, along with the prescribed proof of identity documents having the correct name. In case of joint holders in a demat account the request should be signed by the holder in whose name the correction is required to be carried out.
- b) The minor correction in name will include following types of cases:
 - i. Correction of spelling mistakes, if any.
 - ii. Expansion of the name by incorporating the fully expanded name and/or addition of middle name.
 - iii. Abbreviation of name.

⁴⁸ Reference: CDSL/OPS/DP/POLCY/2019/17 dated January 9, 2019



- c) DP should ensure to obtain a confirmation from the demat account holder that it is not a change in name of the individual demat account holder[s] for any reason such as marriage, divorce, court order.
- d) If the individual demat account holder changes the spelling of his/her name for any reason including for numerology, etc., it will be considered name change of the BO and will not be treated as correction in name.
- e) DPs are advised to carry out the necessary due diligence while processing such requests and verify that the request for correction in name is received from the same person and ensure that there is no change in name of the BO.

2.1.3 Updation of New Bank Account Numbers

- a) DPs are advised to inform their BOs / clients to update the new bank account numbers in their demat accounts at the earliest, failing which, electronic transfers with old account numbers will be rejected at the ECS centre level itself.⁴⁹
- b) DPs should note that if the new bank account number is to be updated due to the Member Bank's migration to the Core Banking Solution [CBS] platform, the requirement of obtaining an Account Modification Form has been waived.
- c) The new bank account number may be updated based on the notice/letter received from the Bank. All other modifications to bank details should be effected as per SEBI guidelines and CDSL's operating instructions.

2.2 Updation of the demographic details based on a request received from the BO through a secured URL⁵⁰

- a) DPs can update the prescribed demographic details based on a request received from the BO through a secured URL with 'https' with specific login and password provided by the DP through its website.
- b) DPs may permit BOs to modify / update only those details which do not require any documentary proof to be submitted by the BOs to the DPs.

⁴⁹ Reference: CDSL/OPS/DP/1759 dated October 30, 2009

⁵⁰ Reference: CDSL/OPS/DP/POLCY/2532 dated June 30, 2011



- c) For updation of any other details that will require supporting documents as stipulated in DP Operating Instructions such as PAN card, change of address, etc., the existing procedure of BO approaching the DP and submission of Account Modification / Deletion Request form will continue.

2.3 PAN Modification at DP end⁵¹

- a) DP can modify the existing PAN along with correct verification code and applicable reason code. In case of PAN exemption code being entered by the DP, supporting documents have to be uploaded by the DP.
- b) DPs to upload the supporting duly verified copy of PAN.
- c) The PAN modification maker entries done by the DP will be verified by CDSL end. After approval by CDSL the said PAN modification will be updated in demat account and DP will be able to view the same.
- d) If PAN modification request is rejected by CDSL then email will be sent to the registered email ids of DP recorded in CDAS system.
- e) DPs are required to make note the same and also ensure that no email copies are marked to CDSL.

⁵¹ Reference: CDSL/OPS/DP/POLCY/2019/337 dated July 05, 2019



Chapter 3 : Dematerialisation

3.1 Review of rejection of demat requests⁵²

- 3.1.1 DPs are advised to exercise care while processing Demat Requests with regard to set-up details of the DRN and subsequent dispatch of documents to Issuers/RTAs. Rejections of demat requests causes hardship and inconvenience to investors. Therefore, DPs are advised to put in place proper mechanisms for processing of Demat Requests, so as to avoid rejections.

3.2 Demat Request - Change in the name of the Company⁵³

- 3.2.1 CDSL provides data of old and new company names on CDAS. In case share certificates with the old name of companies are received for dematerialisation, the DPs need not reject such requests.
- 3.2.2 This is not applicable for companies that have merged or amalgamated with other companies.

3.3 Processing of request for dematerialization of shares vested with custodians⁵⁴

- 3.3.1 Under some cases, Custodians are appointed under some special Acts such as Trail of Offences Relating to Transactions in Securities Act 1992 (TORTS), Enemy Property Act, 1968 etc. These Custodians are also required to hold shares of listed companies.
- 3.3.2 In such matters, the Custodians may be treated as holder/members in the Register of Member of the company. The Custodians may also hold such shares in a dematerialized form in terms of Depositories Act, 1996.
- 3.3.3 If any RTA/Company receives an application from such Custodians for dematerialization of shares, it is clarified that:
- The Regulation 40(1) of Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, which disallows transfer of physical shares from April 01, 2019, will not be applicable in such matters.
 - The shares after dematerialization may be credited to the demat account of such custodians.

⁵² Reference: CDSL/OPS/DP/857 dated March 02, 2007

⁵³ Reference: CDSL/OPS/DP/606 dated November 17, 2005

⁵⁴ Reference: CDSL/OPS/DP/POLCY/2021/395 dated September 07, 2021



Chapter 4 : Settlements

4.1 Issue of Instruction Slips

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to Issue of Instruction Slips shall require to be complied with:

- 4.1.1 DPs should ensure that details of DIS issued to BOs are entered (online /upload) in CDSL system. All such DIS should comply with the standardization requirements as specified in CDSL.⁵⁵

4.2 Monitoring of DIS

- 4.2.1 All transactions except for transactions received through “easiest” from BO or Clearing Members (CMs), TRUST and digitally signed instructions (i.e. electronic instructions) DIS serial number will be required to be entered along with transactions, failing which the transactions will fail. DIS details so entered will be verified against DIS issuance details in the system.⁵⁶
- 4.2.2 DPs should capture details of undelivered DIS serial numbers in CDAS on receipt of such information.⁵⁷

4.3 Scanning of DIS⁵⁸

- 4.3.1 The DIS should be scanned and stored in a file by the end of next working day after it is entered in the depository system by the Main DP/Live connected Branch DP. The scanned image of DIS should be legible.
- 4.3.2 If any DIS is required to be rescanned, both images (originally scanned & rescanned) should be stored.

⁵⁵ Reference: CDSL/OPS/DP/POLCY/4664 dated August 27, 2014

⁵⁶ Reference: CDSL/OPS/DP/POLCY/5577 dated November 24, 2015

⁵⁷ Reference: CDSL/OPS/DP/POLCY/5327 July 20, 2015

⁵⁸ Reference: CDSL/A,I&C/DP/POLCY/4685 September 04, 2014 and CDSL/A,I&C/DP/POLCY/4729 September 25, 2014



- 4.3.3 Storing of scanned images is not mandatory, since the scanned images need to be uploaded by the DP to CDSL.
- 4.3.4 The DP should scan and store each DIS separately with the file name.
- 4.3.5 In case of DIS with annexures, each page of annexure should also be separately scanned along with the DIS. The annexures / computer print-outs should be scanned without compromising the legibility.
- 4.3.6 If Date and time receipt stamp is affixed on the back side of the DIS by the DP, the DP needs to scan back side of DIS containing receipt stamp/acknowledgement stamp. DIS serial number should be mentioned along with the stamp on the back side of the DIS before scanning the back side of DIS containing receipt stamp.
- 4.3.7 In case of instructions executed on the basis of fax copy of DIS received from BOs, the original DIS should bear either on the front or back of the DIS a stamp stating that “This is a hardcopy of DIS with serial no. ----- of the fax transmission to you, transmitted on _____ day of _____ month of _____ year.” If the above stamp is affixed on back side of the DIS, then DP should scan both the sides of DIS and store the image. After receipt of Original DIS of Fax instruction, it should be scanned and image should be stored. The Original DIS should be scanned by the end of the next working day of the date of receipt of DIS. If original DIS is lost in transit, the DP should take confirmation from the BO for having issued that DIS.
- 4.3.8 In case of DIS used by a BO in a dormant account, if the details of verification are written on the back-side of the DIS, the DP should scan both the sides of DIS.
- 4.3.9 All scanned DIS with the file name as stated above should be uploaded to CDAS system by the end of next working day of set up of transaction.
- 4.3.10 CDSL may conduct the inspection of DPs either offsite or onsite. Offsite inspection would be conducted on the basis of scanned image of DIS. However, during onsite inspection, if required/demanded by inspecting official, the original DIS should be made available for verification.
- 4.3.11 The original DIS should be easily retrievable and made available for verification at any point of time as may be required by CDSL or any other Statutory /Regulatory body.



4.3.12 The concurrent auditors shall verify that the DP does scanning of all DISs within a stipulated time and comment to that effect in the concurrent audit report.

4.4 Off market transactions

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to Off market transactions shall require to be complied with:

- 4.4.1 If the Off-market transaction is for consideration, the amount should be mentioned. If there is no consideration involved, then reason should be furnished under options given therein.⁵⁹
- 4.4.2 The above-referred details of transactions may be taken on the face of the DIS or on a separate sheet duly signed by the account holders.
- 4.4.3 It has been decided to implement uniform / standardized reason codes for off-market transfers by both depositories, to provide an audit trail of reasons associated with such transfers as a risk mitigation measure. DPs are advised to note that reason code is mandatory in case of off market transactions (within CDSL or Inter Depository)⁶⁰
- 4.4.4 One Time Password (OTP) authentication by BO would be mandatory for all off-market transfers (i.e. Transfer of securities within CDSL as well as inter- depository transfer).⁶¹
- 4.4.5 In order to ensure that the off-market transfer is indeed for the purported reason as declared by the account holder(s) at the time of off-market transfers, system level validation is being implemented by Depositories for off-market transfers.⁶² DPs are requested to take note of the validations elaborated in the Communiques and ensure due diligence to avoid non-execution of off-market transactions.⁶³

⁵⁹ Reference: CDSL/OPS/DP/989 dated November 13, 2007

⁶⁰ Reference: CDSL/OPS/DP/SYSTEM/6085 dated August 17, 2016 and CDSL/OPS/DP/SYSTEM/2019/352 dated July 15, 2019

⁶¹ Reference: CDSL/OPS/DP/POLCY/2020/447 October 14, 2020

⁶² Reference: CDSL/OPS/DP/SYSTEM/2021/569 December 15, 2021

⁶³ Reference: CDSL/OPS/DP/SYSTEM/2022/340 June 20, 2022



4.5 Acceptance of Delivery Instructions through online Portal of DPs / Stock Brokers⁶⁴

4.5.1 SEBI has examined the facility of accepting Delivery Instructions through Online Portal of DP/Stock Broker which has been enabled by CDSL as e-DIS and its process of seeking authorizations/mandate.

4.5.2 e-DIS facility: The facility of e-DIS has to be true to its label and should:

- a) Necessarily capture all details that are otherwise being captured in physical DIS, including settlement number and actual quantity to be transferred in case of on-market transfers.
- b) Be an instruction toward actual transfer of securities to meet obligation for a single settlement number/date.

4.5.3 Pre-trade authorisation/Mandate: The following shall be required to be ensured:

- a) The mandate should be received from BO authorising the concerned DP/Stock Broker to transfer specific securities for meeting on-market settlement obligation only.
- b) Such mandate should necessarily pertain to a single settlement number/settlement date.
- c) BO shall be required to authorise each mandate valid for a single settlement number/settlement date, by way of OTP and TPIN/Password, both generated at Depositories end.
- d) Prior to executing actual transfer of securities based on details provided by DP/Stock Broker, Depositories need to match and confirm the same with mandate provided by client as well as client-wise net delivery obligation arising from the trade executed on exchange, as provided by Clearing Corporation to Depositories for each settlement date.
- e) Securities transferred on basis of mandate provided by BO should be credited only to BO's trading member pool account.
- f) DP/Stock Broker providing this facility have enabled its BO to revoke / cancel the mandate provided by it.

4.5.4 DP/Stock Broker providing this facility shall ensure that mandate provided by BO adheres to following requirements:

- a) The mandate provided by client should:
 - i. Be in favour of the concerned SEBI registered intermediary only.

⁶⁴ Reference: CDSL/OPS/DP/SETTL/2021/54 dated February 08, 2021



- ii. Not provide the authority to transfer the mandate in favor of any assignees of the concerned DP/Stock Broker.
 - iii. Require the DP/Stock Broker to return the securities to BO(s) that may have been received by them erroneously or those securities that it was not entitled to receive from the BO(s).
- b) The mandate provided by BO shall not facilitate DP/Stock Broker to do the following:
- i. Transfer of securities for off-market trades.
 - ii. To execute trades in the name of BO without BO's consent.
 - iii. To open an email ID on behalf of the BO for receiving relevant communications.
 - iv. Prohibit to issue DIS to BO.
 - v. Prohibit BO from operating the account.
- 4.5.5 DPs are also informed to note of the following clarifications as issued by SEBI to both depositories with respect to process of seeking pre-trade authorization /mandate:
- a) It is mandatory for the BO to specify the settlement number/settlement date at the time of providing the pre-trade authorisation/mandate.
 - b) Mandate provided for multiple ISINs shall not lapse if the debit is effected only for one particular ISIN, however such mandate shall be valid only for a particular settlement number/date as specified in the mandate.
 - c) Mandate received from BO should only be for a single settlement number/date as provided by BO. The same cannot be exercised before or after the given settlement date.
- 4.5.6 DPs are advised to follow the procedure for Acceptance of Delivery Instructions through online Portal of DP/ Stock Broker as mentioned in the communique along with further clarifications issued regarding the same.
- 4.6 Using e-DIS (Electronic Delivery Instructions)⁶⁵**
- 4.6.1 e-DIS facility shall be allowed to be used by all type of investors subject to the DPs are registered for e-DIS facility.

⁶⁵ Reference: CDSL/OPS/DP/GENRL/2021/446 dated October 04, 2021



- 4.6.2 DPs should have suitable checks, measures in place, must take the onus and responsibility to ensure that the documents collected are in order as per guidelines mentioned in the CDSL bye laws, Operating Instructions, e-DIS Process Flow and e-DIS registration Form issued from time to time.
- 4.6.3 Further, the authorized signatories; if more than one, would have to give a confirmation to the DP of agreeing to the usage of the Email ID and Mobile Number on which the authentication details including TPIN and OTP will be sent for authenticating the transactions (referred as e-mandate)
- 4.6.4 The following checks and balances are required to be taken care during the processing of e-DIS transactions:
- a) The investor is required to use the DP/Stock Broker Portal to put through the request for sale.
 - b) The information on the request for sale should flow to CDSL through an API and thereafter approved by the account holder through CDSL generated TPIN and OTP.
 - c) CDSL approves or rejects the request based on the TPIN and OTP entered by the demat account holder.
 - d) When the e-DIS transaction is entered in the CDSL system, the CDSL system checks for the corresponding approval received from the investor through e-mandate which is authenticated by investor itself for e-DIS transactions and is processed based on the availability of balances.
 - e) The transactions are earmarked immediately on entry of instructions, but balance is debited only after matching of the e-DIS transaction with corresponding UCC wise net delivery obligation received from the Clearing Corporation.
 - f) The basic checks of ensuring multiple e-signs are obtained where relevant documents depending on the type of account.

4.7 Block Mechanism in demat account of clients undertaking sale transactions⁶⁶

- 4.7.1 When the client intends to make a sale transaction, shares will be blocked in the demat account of the client in favour of Clearing Corporation. If sale transaction is not executed, shares shall continue to remain in the client's demat account and will be unblocked at the end of the T day. Thus, this mechanism will do away with the movement of shares from client's demat account for early pay-in and back to client's demat account if trade is not executed.

⁶⁶ Reference: CDSL/OPS/DP/POLCY/2021/314 dated July 19, 2021



4.7.2 Process flow for Block Mechanism:

- a) The securities lying in client's demat account will be blocked either by client himself using depository's online system or eDIS mandate or through depository participant based on physical DIS given by client or Power of Attorney (POA) holder.
- b) Depositories may keep block on the securities in client's demat account in respect of Intra or Inter depository transfer instruction till pay-in day. The blocked securities will be transferred only after checking against the client level net delivery obligation received from CCs.
- c) Depositories will provide the details of transfer instructions viz., UCC, TM ID, Exchange ID etc. to CCs for clients to avail EPI benefit.
- d) CC will match the client level net obligations with the Block details provided by depositories and CC will provide EPI benefit to client if the client level net obligation exists for that client.

4.7.3 Matched orders:

- a) In case of matched orders, block securities will be debited from Client's demat account and will be credited to linked TM Pool account upto pay-in day. TM shall further transfer such securities to CM Pool account.
- b) TM shall not transfer the securities to any other pool account other than CM pool account mapped to the TM account. Pool to Pool transfers except TM pool to CM pool shall not be permitted.
- c) Inter-settlement shall not be allowed from TM Pool account and CM pool account.
- d) Securities lying in CM pool account will be delivered in settlement process on the Pay-in date. If TM Pool Account is also mapped as a CM Pool Account, then, securities lying in such TM/CM Pool Account can also be delivered in the settlement process.

4.7.4 Unblocking of Securities:

- a) After receiving client level net obligations on T day from CCs, depositories will match the Intra or Inter depository transfer instruction details with CC obligation details based on UCC, TM ID, CM ID, Exchange ID, etc.
- b) In case of unmatched orders, CCs shall upload cancellation of Block instruction on T day so that securities are unblocked and become free in client's demat account on T day itself.
- c) Broker or client shall not be allowed to unblock securities if EPI benefit is provided by CC to client for the same.



4.7.5 **Margining of Trades:**

- a) When the client intends to block securities for a sale transaction, shares will remain blocked in favour of CC. If securities are blocked in favour of CC, then all Margin would be deemed to have been collected and penalty for short/non-collection of margin including other margins shall not arise.
- b) Blocking shall be on 'time basis' and would mean if the order is not executed by the end of the T day, the block shall be released.

4.7.6 The block mechanism shall not be applicable to clients having arrangements with custodians registered with SEBI for clearing and settlement of trades.⁶⁷

4.7.7 UCC will be mandatory for all type of pay-in transactions. If setup quantity (qty) of pay-in transaction (txn) is more than the obligation qty then available balance to the extent of obligation qty will be considered for pay-in.⁶⁸

4.7.8 DPs/TMs/CMs will also require to mandatorily provide UCC details in TM/CM Pool to TM/CM Pool on-market and, inter-settlement. Details of these txns will get validated with CC delivery obligation for the UCC-Settlement ID-CMID combination of target TM/CM Pool account.

4.7.9 DPs/TMs/CMs will also require to mandatorily provide UCC details in EP txn from TM/CM Pool account. Details of these txns will be validated with CC delivery obligation for the UCC-Settlement ID-CMID provided in the txn.

4.8 **Validation of Instructions for Pay-In of Securities from Client demat account to Trading Member (TM) Pool Account against obligations received from the Clearing Corporations⁶⁹**

4.8.1 Depositories, prior to executing actual transfer of the securities for Pay-In from client demat account to TM Pool account, shall validate the transfer instruction received through any of the available channels for the purpose of Pay-in, i.e. either initiated by clients themselves or by the Power of Attorney (POA) / Demat Debit and Pledge Instruction (DDPI) holder against the client-wise net delivery obligation received from CCs.

4.8.2 For Early Pay-In transactions, the existing facility of Block mechanism shall continue.

⁶⁷ Reference: CDSL/OPS/DP/P OLCY/2022/627 dated October 28, 2022

⁶⁸ Reference: CDSL/OPS/DP/ SETTL/2022/638 November 03, 2022

⁶⁹ Reference: CDSL/OPS/DP/P OLCY/2022/540 dated September 21, 2022



4.8.3 **Validation of transfer instruction details with CC obligation details**

- a) Depositories receive the debit instruction for the purpose of Pay-In, given either by client himself using depository's online system or eDIS mandate or through depository participant based on physical DIS / digitally signed DIS given by client or POA / DDPI holder.
- b) CCs shall provide client-wise net delivery obligations on T day to the depositories.
- c) Based on the obligation data provided by CCs, Depositories shall validate the depository transfer instruction details with CC obligation details based on UCC, TM ID, CM ID, Exchange ID, ISIN, quantity, settlement details etc.

4.8.4 **Matched instruction:**

In case of matching of all details like UCC, TM ID, CM ID, ISIN, quantity, settlement details etc. of the transfer instruction with the obligation data, the instruction shall be carried out by the Depositories and such securities will be debited from client's demat account and credited to linked TM Pool account on or before the settlement day.

4.8.5 **Unmatched instruction:**

- a) In case of discrepancies in details like UCC, TM ID, CM ID, ISIN etc., between instruction and obligation, such transfer instructions will be rejected by the depositories.
- b) In case of discrepancies in quantity of securities between instruction and obligation, the following shall be noted:
 - i) If the quantity in instruction is less than the obligation provided by CC, then the instruction will be carried out by the depositories.
 - ii) If the quantity in instruction is more than the obligation provided by CC, then the instruction will be partially processed by the depositories (i.e., upto the matching obligation quantity).

4.8.6 **Trades Confirmed by Custodians:**

This process shall not be applicable to clients having arrangements with custodians registered with SEBI for clearing and settlement of trades.

4.8.7 UCC details of the clients undertaking sale transactions would be mandatory for all types of pay-in transactions. UCC details mentioned in the transaction would be validated with UCC details linked to the demat account of the client and transaction would be taken for processing only if UCC details matches. Payin transactions without UCC details or invalid details would be rejected and would not be considered for further processing.⁷⁰

⁷⁰ Reference: CDSL/OPS/DP/S ETTL/2022/462 August 12, 2022 and CDSL/OPS/DP/SETTL/2023/60 January 25, 2023



4.9 Handling of Clients' Securities by Trading Members (TM) / Clearing Members (CM)⁷¹

4.9.1 CDSL has introduced a new pledge reason code for auto pledge transactions for client unpaid securities pledge transactions viz. 'CUSPA Pledge'. The above-mentioned pledge reason code will be captured automatically at the time of creation of pledge in favour of CUSPA.⁷²

4.9.2 Transfer of Pay-out Securities to Unpaid Clients:

- a) Pay-out securities can be transferred to the demat account of the respective clients directly from the TM/CM Pool Account within one working day of the pay-out.
- b) Unpaid securities (i.e., the securities that have not been paid for in full by the client), such securities can be transferred to the demat account of the unpaid client in the following manner.
 - i. While transferring pay-out securities by TM/CM to the unpaid client, entering Transaction Identifier (i.e., transfer for unpaid client), UCC details, CUSPA will be mandatory and can be a part of the annexure to existing DIS.
 - ii. On successful validation of UCC details entered in the transaction vis-à-vis UCC details linked to the demat account of the client, securities shall be credited in the demat account of unpaid client and simultaneously an auto pledge instruction will be setup from demat account of unpaid client in favor of the corresponding CUSPA of a TM/CM. Hence such unpaid securities will be reflected under 'Pledge' balance in the demat account of unpaid client and 'Pledgee' balance will be reflected in CUSPA.

4.9.3 Release of Securities if Unpaid Client Fulfills its Funds Obligation:

- a) If unpaid client fulfills its funds obligation within five trading days after the payout, TM/CM shall release the pledge so that the securities are available to the client as free balance. TM-CM can unpledge the securities with partial or full quantity.
- b) DPs may obtain the CUSPA Unpledge Request Form, as prescribed by CDSL.

⁷¹ Reference: CDSL/OPS/DP/S ETTL/2023/151 dated March 09, 2023

⁷² Reference: CDSL/OPS/DP/SETTL/2023/208 dated March 31, 2023



4.9.4 Confiscation / Invocation of Securities if Unpaid Client doesn't Fulfill its Funds Obligation:

- a) If the client does not fulfill its funds obligation, TM/CM can dispose off such unpaid securities in the market within five trading days after the pay-out. As per the SEBI guidelines, TM/CM, before disposing of the securities, is required to give an intimation (email /SMS) to the client, one trading day before such sale.
- b) Such unpaid securities will be disposed off by TM/CM by executing a sale transaction with UCC details on the exchange platform and then executing a 'Confiscation-cum Early Payin (EP)' transaction in CDSL system. DPs shall obtain the 'Confiscation-cum-Early Pay-in' form as prescribed by CDSL.
- c) DPs are advised to accept and execute 'Confiscation-cum-Early Pay-in' transactions latest by 09:45 am on pay-in day i.e., T+1 day. DPs are requested to take note of 'Confiscation cum-Early Pay-in' request accepted and entered after 09:45 am on pay-in day i.e., T+1 will be processed only on best effort basis. CDSL will not be responsible for any failure in processing of 'Confiscation-cum-Early Pay-in' request accepted and executed after 09:45 am on pay-in day i.e., T+1 day.

4.9.5 No Action on Pledged Securities of Unpaid Clients by TM/CM within Seven Trading Days after Pay-out:

- a) In case, pledged securities with respect to unpaid clients is neither invoked/confiscated nor released/unpledged within seven trading days after the pay-out (i.e., till the EOD of seventh trading day), the pledge on securities shall be auto released/unpledged and the securities shall be made available in the client account as free balance.
- b) DPs may note that no prior intimation will be sent by CDSL to TM/CM/DP about the auto unpledge of securities due to no-action from TM/CM.

4.9.6 The unpaid securities pledged in demat account of unpaid client shall not be considered for the margin obligations of the client.

4.9.7 The payment of stamp duty will be applicable for CUSPA pledge invocation instruction same as normal pledge invocation instruction.



4.10 Tagging of Demat Accounts of stock brokers⁷³

4.10.1 DPs are advised to refer to SEBI Circular no. SEBI/HO/MIRSD/MIRSD2/CIR/P/2016/95 dated September 26, 2016 wherein SEBI has informed guidelines regarding enhanced supervision of stock brokers/depository participants.

4.10.2 Uniform nomenclature is to be followed by stock brokers for Naming/Tagging of Demat Accounts and the reporting of such accounts to the Stock Exchanges/Depositories to reflect the purpose for which these demat accounts are being maintained.

4.10.3 Stock Brokers (SB) are required to maintain demat accounts only under the following 5 categories:

Sr. No.	Demat Account Category	Purpose of Demat Account
a.	Proprietary Account	Hold Own Securities
b.	Pool account	Settlement Purpose
c.	Client Unpaid Securities Pledge Account	Hold Pledged Unpaid Securities of Client
d.	Margin Pledge and Unpledge Account for Client Pledged Securities	For Margin obligations to be given by way of Pledge/Re-pledge
e.	Client Securities under Margin Funding Account	Hold funded securities in respect of margin funding

4.10.4 DPs are advised to refer the relevant the SEBI Circulars and CDSL Communiques in respect of discontinuation of below-mentioned category of broker accounts.

Sr. No.	Demat Account Category (to be discontinued)	Purpose of Demat Account
a.	SB - Client Account	To hold client's securities
b.	SB - Collateral Account	For depositing securities collateral with the Clearing Corporation
c.	SB - Margin Trading Account	To provide margin trading facility
d.	Client Unpaid Securities Account	Hold Unpaid Securities of Client

⁷³ Reference: CDSL/OPS/DP/POLCY/6160 dated September 29, 2016, CDSL/OPS/DP/POLCY/2022/342 dated June 21, 2022; CDSL/OPS/DP/POLCY/2022/368 dated June 28, 2022 and CDSL/OPS/DP/POLCY/2022/427 dated July 28, 2022



4.10.5 Stock brokers maintaining demat accounts other than the above-mentioned categories would be considered as ‘untagged’ accounts. All demat accounts of stock brokers which are untagged need to be appropriately tagged. All ‘untagged’ accounts would be marked as ‘Frozen for Debit and Credit’. Only credits arising out of Corporate Action would be allowed in the said accounts. If any tagging is required to be done in ‘untagged’ accounts or securities to be transferred to the client account from the ‘untagged’ accounts, then the brokers will be required to approach corresponding Stock Exchange/s. Based on the instructions received from the Stock Exchanges, CDSL will unfreeze the account and then broker can execute sub-status modification or transfer of securities to the client account as the case may be.

4.10.6 ‘Untagged’ demat accounts which are used exclusively for banking activities by the brokers which are also banks are exempted from the category of ‘untagged’ accounts and the guidelines mentioned in the aforesaid SEBI circular shall not apply to said exempted ‘untagged’ accounts. To avoid freezing of such banking activity accounts DPs are requested to inform details of said accounts to CDSL.

4.11 Execution of ‘Demat Debit and Pledge Instruction’ (DDPI) for transfer of securities towards deliveries / settlement obligations and pledging / repledging of securities

4.11.1 The client may use the DDPI or opt to complete the settlement by issuing physical Delivery Instruction Slip (DIS) or electronic Delivery Instruction Slip (eDIS) themselves.⁷⁴

4.11.2 For the execution of the DDPI for fulfilling delivery / settlement obligations, prior to executing actual transfer of securities based on details provided by stock broker/stock broker and depository participant, the Depositories shall ensure matching and confirming the transfer of securities with client-wise net delivery obligation arising from the trade executed on the exchange, as provided by the Clearing Corporation to Depositories for each settlement date.

4.11.3 Securities transferred on the basis of the DDPI provided by the client shall be credited to client’s TM pool account / CM pool account / demat account of clearing corporation, as the case may be. The DDPI provided by the client shall be registered in the demat account of the client by TM /CM.⁷⁵

⁷⁴ Reference: CDSL/OPS/DP/POLCY/2022/194 dated April 05, 2022

⁷⁵ Reference: CDSL/OPS/DP/P OLCY/2022/585 dated October 7, 2022



Chapter 5 : Statement of Accounts

5.1 Statement of Accounts in case of PMS (Portfolio Management Services) clients and BSDA Accounts

- 5.1.1 In case of PMS (Portfolio Management Services) clients, Portfolio Manager's address cannot be captured as correspondence address. However, the transaction statements may be sent / made accessible to both – the portfolio manager and its client.⁷⁶
- 5.1.2 In respect of BSDA Accounts with zero balance and nil transactions during the year, DP shall send at least one annual physical statement of holding to the stated address of the BO even after the account has remained in such state for one year. The DP shall inform the BO that the dispatch of the physical statement may be discontinued for the account which continues to remain zero balance even after one year.⁷⁷

⁷⁶ Reference: CDSL/OPS/DP/1622 dated June 22, 2009

⁷⁷ Reference: CDSL/OPS/DP/POLCY/4546 dated July 01, 2014



Chapter 6 : Pledge

6.1 Pledge Reason code and capturing of Ultimate Lender details for Trusteeship Company⁷⁸

6.1.1 DPs need to capture the Ultimate lender details for the pledgee accounts of sub type “Debenture Trustee” and “Trusteeship Company”. Atleast one name and PAN needs to be captured in Ultimate lender master for pledgee of type “Debenture Trustee” and “Trusteeship Company” without which pledge will not be allowed to setup. CDSL has compiled a master list of ultimate lenders containing code and name of the ultimate lenders. DPs need to update the PAN of ultimate lenders and the pledgee demat account in the ultimate lender master. Trustees need to open separate demat accounts for separate set of ultimate lenders before pledge setup.

6.1.2 Further, Pledge reason code from the list given below must be captured by DP for each pledge setup in the system.⁷⁹

- i. Collateral -Debt issuance by Co./Grp Co.
- ii. Collateral for loan by Company/Group Co.
- iii. Collateral for loan by the Third Party
- iv. Margin Pledge/MTF for Exchange Trade
- v. Personal use by promoters and PACs

⁷⁸ Reference: CDSL/OPS/DP/POLCY/2022/451 dated August 08, 2022

⁷⁹ Reference: CDSL/OPS/DP/POLCY/2022/385 dated July 05, 2022



Chapter 7 : Freeze / Unfreeze

7.1 Freeze and Unfreeze instruction using easi/easiest login⁸⁰

- 7.1.1 DPs are advised to take note of the facility provided by CDSL to easi/easiest users to execute 'Freeze' and 'Unfreeze' transaction without submitting freeze/unfreeze instruction to the Depository Participant.
- 7.1.2 DPs are not required to obtain a freeze/ unfreeze request form for the freeze/ unfreeze request set up by the BOs from their easi/easiest login.

7.2 Framework for automated deactivation of demat accounts with inadequate Know Your Customer (KYC) details⁸¹

- 7.2.1 Demographic details of a client form an important aspect of KYC procedure. DPs are required to maintain updated client information including their addresses. DPs are also required to update the same with the Depository. However, in some cases, the address of demat account holder(s) are not updated. As a result, during the course of any enforcement proceedings, when SEBI issues any notices etc., on such addresses, at times, the same remains unserved.
- 7.2.2 The framework for delivery of Show Cause Notice (SCN)/Order issued by SEBI and Freezing of demat accounts in case of the SCN/Order remains unserved is as under:
- Upon receipt of instruction from SEBI to deliver any SCN/Order issued by SEBI, CDSL shall forward the same to the respective DPs via email for physical delivery to the Noticee /Addressee.
 - DP shall physically deliver the said SCN/Order to the Noticee/Addressee at the address(es) available with the DP.
 - DP shall also simultaneously email the scanned copy of the SCN / Order to the demat account holder(s).
 - In case of joint demat account(s), the DP shall contact the Noticee/Addressee through the joint account holders for delivery of SCN/Order simultaneously by following the same process.
 - DP is required to obtain duly signed physical acknowledgement of receipt of said SCN/Order from the Noticee /Addressee or its authorised representative in the format provided by CDSL. and forward the scanned copy of the signed acknowledgement

⁸⁰ Reference: CDSL/OPS/DP/EASI/4768 dated October 17, 2014

⁸¹ Reference: CDSL/A,I&C/DP/POLCY/2022/515 dated September 08, 2022 and CDSL/AI&C/DP/POLCY/2022/683 dated November 29, 2022



to CDSL at email id: cdsl.ews@cdslindia.com with subject “Delivery of show cause notice/order of SEBI and updation of KYC details in the Depository system” within 2 working days from receipt of acknowledgement. Further, the DP shall also send the original signed acknowledgement by courier / speed post to CDSL at Surveillance Department, Central Depository Services (India) Limited, Marathon Futurex, ‘A’ Wing, 25th Floor, Mafatlal Mills Compound, N. M Joshi Marg, Lower Parel (E), Mumbai-400013, within 2 working days from receipt of acknowledgement.

- f) In case of failure to obtain physical acknowledgement of delivery of show cause notice/Order from the demat account holder(s) by the DP and submission of the same, CDSL shall freeze (For Debit and Credit, except for corporate actions) such demat account holder(s) under freeze reason ‘SEBI SCN / Order Not Delivered/Acknowledged’. If the demat account holder(s) is a joint account holder relating to a joint demat account, then CDSL shall freeze such joint demat account also. Further, no new demat accounts can be opened under the said PAN.
- g) For information regarding the list of Frozen demat account holder(s), DPs are requested to refer the following link:
<https://www.cdslindia.com/downloads/investors/SCNPANList/List%20of%20PAN%20Frozen%20on%20account%20of%20non-delivery%20of%20SCN-Orders.pdf>
- h) If the address of the Noticee/Addressee is not matching with the address captured in the demat account, then DP shall update the latest KYC details of the said demat account holder(s) as per the extant norms in CDSL system and also with respective KRA based on the documents obtained from the Noticee/Addressee.
- i) Upon updating the KYC details in the CDSL system and respective KRA, DP shall submit a confirmation along with requisite supporting KYC documents received from Noticee/Addressee via email at email id: cdsl.ews@cdslindia.com with subject “Delivery of show cause notice/order and updation of KYC details in the Depository system”.
- j) If the same Noticee/Addressee (as per PAN) is having demat account with other DPs, then the respective DP shall update the address in the KYC records as per extant norms based on intimation from CDSL.

7.2.3 Process to be followed where DP is not able to complete physical delivery of SCN/Order to the Noticee/Addressee or obtain acknowledgement:

- a) DP shall inform CDSL about the non-delivery of SCN/Order to the Noticee/Addressee or failure to obtain acknowledgement within the date specified by CDSL in its communication.
- b) CDSL shall thereafter share the information of non-delivery status with other MIIs and if required, steps would be taken for deactivation of concerned demat account(s) of Noticee/Addressee within 5 working days from the last unsuccessful delivery



report.

- c) CDSL shall freeze (For Debit and Credit, except for corporate actions) such demat accounts under freeze reason 'SEBI SCN/Order Not Delivered/Acknowledged'.
- d) If the Noticee / Addressee is a joint account holder relating to a joint demat account, then CDSL shall freeze such joint demat account also.

7.2.4 Steps for Reactivation of the demat account of Noticee / Addressee: If the Noticee/Addressee subsequently approach the DP for reactivation of demat account, the below mentioned procedure shall be followed by the concerned DP:

- a) Obtain following documents from the Noticee/Addressee: (i) Copy of updated proof of address; and (ii) Signed acknowledgement of receipt of SCN/order issued by SEBI.
- b) Update KYC records based on the updated proof of address in CDSL system and respective KRA as per extant norms.
- c) Forward scanned copy of the signed acknowledgement along with requisite supporting KYC documents received from client to CDSL and confirmation on updation of KYC records of the Noticee/Addressee in the Depository system and respective KRA at email id: cdsl.ews@cdslindia.com with subject "Delivery of show cause notice/order of SEBI and updation of KYC details in the Depository system" within 2 working days from receipt of acknowledgement. Further, the DP shall also send the original signed acknowledgement by courier/ speed post to CDSL at Surveillance Department, Central Depository Services (India) Limited, Marathon Futurex, 'A' Wing, 25th Floor, Mafatlal Mills Compound, N. M Joshi Marg, Lower Parel (E), Mumbai- 400013 within 2 working days from receipt of acknowledgement.
- d) On receipt of above, CDSL, shall verify the signed acknowledgement and if found satisfactory, shall initiate steps for reactivation of all the demat account(s) (including joint account(s)) held within CDSL by unfreezing the demat account(s) for Debit & Credit'.
- e) If the Noticee/Addressee holds more than one demat account with CDSL, then CDSL shall inform the other DPs with whom the other demat account(s) are held about reactivation of demat account of the Noticee/ Addressee.
- f) Based on aforesaid intimation, the other DPs shall update the address in the KYC records as per extant norms.

7.2.5 In an event, where the client wishes to open a new demat account with the DP, the DP would be required to write to CDSL at cdsl.ews@cdslindia.com, to seek the show cause / order copy and provide an acknowledgement. The concerned DP shall then obtain relevant KYC details and update the same with KRA and intimate to CDSL.



Chapter 8 : Account Closure

8.1 Closure of an account due to shifting or transmission within CDSL

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional steps should be taken for transfer of under lock-in securities or securities under inactive ISINs.

8.1.1 Shifting of Account:

- a) DP shall forward a request in prescribed format to the concerned Issuer/RTA along with copies of CMR of the existing and the target account duly stamped and signed for execution of corporate action to effect the transfer of securities. A copy of request in prescribed format should be forwarded to CDSL.

8.1.2 Transmission:

- a) Upon submission of all the required documents by the legal heir/legal representatives of the deceased Client, as prescribed by the CDSL/SEBI for Transmission, the DP shall verify the documents and forward a request in prescribed format to the concerned Issuer/RTA for execution of corporate action to effect the transfer. A copy of request in prescribed format should be forwarded to CDSL.⁸²

8.2 Guidelines for online closure of demat accounts⁸³

- 8.2.1 Client shall be entitled to close the demat account through online mode without mandatorily giving any reasons to the DP. Clients shall not be restricted from requesting, through online mode or offline mode, for the closure of demat account maintained with the DP, subject to the compliance requirements as stipulated by SEBI / Depository from time to time.
- 8.2.2 Online closure of demat accounts shall be made available for the clients who have opened their accounts offline or online, by the DPs that provide various depository related services in online mode. Those DPs which do not provide any services online and do not open accounts online may not be required to offer online closure of demat accounts.

⁸² Reference: CDSL/OPS/DP/POLCY/2445 dated May 12, 2011

⁸³ Reference: CDSL/OPS/DP/POLCY/2021/311 dated July 16, 2021



- 8.2.3 Account closure for account with balance shall be done only through web portal/app of DP through secured access by way of client specific user ID and password (in case of internet clients) and the request send through emails, SMS, other messaging apps, etc. shall not be entertained by the DP. As the KYC process requires e-sign post which demat accounts can be opened by the DP, for online closure of accounts with balance also, client shall be required to e-sign the form (using Aadhaar based online electronic signature service) to be verified by the DP in accordance with guidelines as stipulated by SEBI/Depositories from time to time.
- 8.2.4 In case of clients having demat accounts with nil balances can be closed by the DPs on the basis of emails received from the registered email ID of the demat account holder.
- 8.2.5 Once the application for closure of demat account is received, the DP shall intimate to the client on registered email id and/or mobile number (on both if available) about the receipt of closure request. A confirmation regarding the request made shall be sought from the client by way of OTP sent on the email id and/or mobile number updated in its source account (to be closed account).
- 8.2.6 The request for demat account closure shall include target account details (in case of request for closure of demat account having security balances is made) where the client intends to shift the securities.
- 8.2.7 Client would have to upload the scan/photograph of his/her signature alongwith Client Master Report (CMR) of the target account digitally signed by official of the target DP (CMR applicable in case of account having security balances). Filled Account Closure form alongwith uploaded ink-signature of the client and CMR as uploaded, would be displayed in one single file to the client, subsequent to which, client shall then be required to e-sign the form (using Aadhaar based online electronic signature service) alongwith the documents and submit the same for further processing. The requirement of obtaining a CMR will be exempted if the DP is able to verify the target demat account details (i.e. sole holder's name and PAN should match perfectly) directly from the Depository electronically.
- 8.2.8 If the DP authorises the request received, the account will get closed in the Depository system. If the DP rejects the client requests received, the DP shall inform the reason for such rejection to the client.



- 8.2.9 In case the target account of the client specified in the account closure form is not its own account i.e. not the same PAN both in source and target accounts, as per the extant requirements, it will be necessary for the client to submit an off-market transfer instruction delivery instruction slip for execution of such transfers along with the requirement of entering OTP as provided by the Depository.
- 8.2.10 After the closure of demat account by the DP, the same shall be intimated to the client through electronic mode enclosing the CMR & Transaction cum Holding Statement of the closed account.
- 8.2.11 DP shall maintain and store system logs of the closure instructions and e-signed electronic requests (uneditable) received in electronic form in a secured manner and the same shall be subject to 100% internal audit.
- 8.2.12 Notwithstanding any such closure of demat account, all rights, liabilities and obligations of the parties arising out of or in respect of transactions entered into prior to the closure of demat account shall continue to subsist and vest in / be binding on the respective parties or his/its respective heirs, executors, administrators, legal representatives or successors, as the case may be.
- 8.2.13 The above process shall be applicable in case of individual client accounts with single holder (without pledge/freeze/pending demat requests balances) and the closure requests accepted through above mechanism shall be considered as a valid client request and DPs/Depository shall not be held liable for acting on such requests.
- 8.2.14 DPs shall inform their clients regarding the availability of facility for online closure of demat accounts through emails, SMS, weekly/fortnightly/monthly newsletters etc. The procedure for online closure of demat accounts shall be prescribed in such communications.



Chapter 9 : Mutual Fund Units

9.1 Destatementization

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines for Destatementization of Mutual Fund units should be complied with

- 9.1.1** DPs shall inform their clients regarding acceptance of statement of accounts (SOA) of earlier date (e.g. quarterly statement) along with demat / remat request form.⁸⁴

9.2 Two-Factor Authentication for transactions in Units of Mutual Funds⁸⁵

- 9.2.1 DPs are advised to refer to SEBI Circular no. SEBI/HO/IMD/IMD-I DOF1/P/CIR/2022/132 dated September 30, 2022, regarding Two-Factor Authentication for transactions in units of Mutual Funds.

- 9.2.2 Accordingly, in case of subscription and redemption of units, Two-Factor Authentication (for online transactions) and signature method (for offline transactions) shall be used for authentication. One of the Factors for such Two-Factor Authentication for non-demat transaction shall be a One-Time Password sent to the unit holder at his/her email/ phone number registered with the AMC/RTA. In case of demat transaction, process of Two-Factor authentication as laid down by the Depositories shall be followed. It is also clarified that in case of mandates/systematic transactions the requirement of Two-Factor Authentication shall be applicable only at the time of registration of mandate/systematic transactions.

9.3 Discontinuation of usage of pool accounts for transactions in units of Mutual Funds on the Stock Exchange Platforms⁸⁶

Pooling of funds and/ or units by stock brokers / clearing members in any form or manner shall be discontinued for mutual fund transactions.

⁸⁴ Reference: CDSL/OPS/DP/MFUND/2021/407 dated September 14, 2021

⁸⁵ Reference: CDSL/OPS/DP/POLCY/2022/567 dated October 3, 2022

⁸⁶ Reference: CDSL/OPS/DP/POLCY/2021/453 dated October 06, 2021



Similar to mechanisms for transactions in mutual fund units by MFDs and IAs, stock exchanges shall put necessary mechanisms in place for stock brokers / clearing members also, to ensure that funds pay-in is directly received by the clearing corporation from the investor account and funds pay-out is directly made to the investor account. Pay-in / pay-out of funds shall not be handled by the stock brokers / clearing members. In the same manner, for both demat and non-demat mode transactions, the units shall be credited and debited directly to/ from the investors' demat account/ folio account without routing it through the pool account of the stock brokers / clearing members. However, for redemption of units held in dematerialised mode, the practice of issuance of Delivery Instruction Slip ('DIS') (physical or electronic) to the Depository Participant to debit the units for delivery to clearing corporation may continue.



Chapter 10 : Internal Controls / Reporting to CDSL

10.1 Appointment of Compliance Officer

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to Appointment of Compliance Officer shall require to be complied with:

10.1.1 The Compliance Officer appointed by the DPs for the main DP office and at their live connected branches should be

- a) an employee of the DP, and
- b) either:
 - 1. a director of the DP, or
 - 2. a graduate with two-year experience in securities market, or
 - 3. a holder of Secondary School Leaving Certificate with five-year experience in the securities market,⁸⁷

10.1.2 The Compliance Officers employed by a DP should obtain Securities Intermediaries Compliance Certification Examination (SICCE) Certification within one year from date of his employment.⁸⁸

10.2 Authorized signatory of DP⁸⁹

10.2.1 DP should register more than one authorized signatory with CDSL for signing important correspondence like contingency set-up, main DP/branch DP right reversals etc.

10.3 Internal Audit and Concurrent Audit⁹⁰

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, SEBI (Depositories and Participants) Regulations, 2018 and Agreement between CDSL and a DP, the following are the additional requirement in respect of Internal Audit and Concurrent Audit:

10.3.1 Online submission of the Internal Audit report should be made to CDSL by 15th May for half year ended 31st March and 15th November for half year ended 30th September.

⁸⁷ Reference: CDSL/OPS/DP/517 dated January 27, 2005

⁸⁸ Reference: CDSL/OPS/DP/POLCY/3549 dated March 13, 2013

⁸⁹ Reference: CDSL/OPS/DP/447 dated August 11, 2004

⁹⁰ Reference: CDSL/AUDIT/DP/POLCY/2022/571 dated October 03, 2022



- 10.3.2 The format of the internal audit report should be in accordance with the Communiqué issued by CDSL from time to time in this regard.
- 10.3.3 The concurrent auditors should conduct the audit of the DPs of Risk Prone Areas of DP Operations (as specified by CDSL from time to time) on 100% basis daily and submit the concurrent audit report to the DP on a monthly basis by the 10th of the following month.⁹¹
- 10.3.4 If any serious non-compliance is reported by the concurrent auditor, the DP should immediately inform CDSL. The DPs should also inform their concurrent auditors that if any serious non-compliance is observed by them during the concurrent audit, the concurrent auditors should report the same to CDSL directly in addition to reporting the same to the concerned DP.
- 10.3.5 The DP should ensure that at least one person conducting the internal and/or concurrent audit of the DP should be NISM certified. The audit report should contain declaration to that effect.
- 10.3.6 If the internal auditor and concurrent auditor of the DP is the same then the consolidated report should be submitted in the format specified by CDSL and in case the auditors are different, then internal audit report should be submitted in the format specified by CDSL along with the report on concurrent audit (CAR) of risk prone areas as per the specified format of CDSL as an attachment to the internal audit report.
- 10.3.7 The DPs will be required to place before their Board the concurrent / internal audit reports and CDSL inspection reports along with the Action Taken Report (ATR) on an on-going basis.
- 10.3.8 The Internal auditors will be required to comment and confirm that DP has placed CDSL inspection report, internal / concurrent audit reports along with the ATRs before the Board meeting in the half yearly internal audit reports.⁹²

⁹¹ Reference: CDSL/A,I&C/DP/POLCY/2022/535 dated September 19, 2022

⁹² Reference: CDSL/A,I&C/DP/POLCY/3770 dated June 27, 2013



10.4 Submission of Compliance Certificate by DPs⁹³

10.4.1 DPs are required to comply with the following:-

- i. The Depositories Act, 1996, SEBI (Depositories and Participants) Regulations, 2018. & its amendments from time to time, Guidelines / Directives / Instructions/circulars issued by SEBI, the Government of India and other Regulatory Bodies from time to time;
- ii. The Bye Laws & Operating Instructions and various communiqués issued by CDSL, from time to time.
- iii. The provisions of Prevention of Money Laundering Act, 2002 and the rules and guidelines issued, there under.

10.4.2 All the DPs are therefore required to submit the 'Compliance Certificate' digitally - signed on half yearly basis to CDSL electronically.

10.4.3 For the half year period from January to June, the Compliance Certificate may be submitted on or before July 31st and for the half year period from July to December to be submitted on or before January 31st of every year.

10.4.4 In case of delay in submission/non-submission of the Half yearly Compliance certificate within stipulated time limit, DPs will be restrained from new account opening if 30 days have elapsed after stipulated time period for submission of the compliance certificate. Matter to be referred to Member Committee if the delay is beyond 60 days from stipulated time period.

10.5 Reporting to CDSL / SEBI⁹⁴

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following are the additional requirement in respect of Reporting to CDSL/SEBI

10.5.1 DPs are required to submit various reports/documents to CDSL within specified time limits. The non-submission or delay in submission of these documents/reports may attract penalty. DPs should ensure that the reports/documents are submitted to CDSL on or before the due date.

⁹³ Reference: CDSL/AUDIT/DP/POLCY/4605 July 28, 2014 and CDSL/OPS/DP/POLCY/6184 dated October 13, 2016

⁹⁴ Reference: CDSL/A,I&C/DP/ POLCY/2535 dated July 01, 2011



10.6 Net Worth Certificate & Audited Financial Statements⁹⁵

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following are the additional requirement in respect of Net Worth Certificate & Audited Financial Statements.

10.6.1 The DPs, seeking extension from Registrar of Companies for holding Annual General Meeting for approval of their annual accounts, are required to submit the copy of approval received from Registrar of Companies to CDSL.

10.6.2 In the past, it is observed that there are some common deficiencies in net worth certificates/AFS submitted by Stock Broker/NBFC/RTA Depository participants. DPs are advised to avoid the following deficiencies while submitting the net worth certificate and AFS.

1. Net worth certificate is not as per the format prescribed under Operating Instruction.
2. Net worth certificate is not submitted in original in case of physical copies being forwarded.
3. Net worth certificate submitted is based on provisional financial statements instead of audited financial statements.
4. Incomplete submission of AFS. The following documents should be part of AFS:
 - a. Auditor's report
 - b. Annexure to the Auditor's reports (CARO)
 - c. Schedules to financial statements
 - d. Accounting Policies & Notes to Accounts
5. The copy of AFS is not attested by the Director of the Company/ statutory auditors.
6. Deferred tax asset, Computer software etc. are not deducted as intangible assets for net worth computation.
7. Statutory Contingent Liabilities are not deducted or partially deducted (50% to be deducted) for net worth computation.
8. If preference shares form part of the 'Share Capital', type of preference shares and the date of redemption is not specified. In case of redemption of preference shares fully during the financial year succeeding 31st March 2023, the same should not be considered for net worth computation. However, in case of partial redemption, the remaining portion of Preference shares which is not being redeemed only can be considered for net worth computation.
9. Bifurcation of computer hardware and software is not provided under the schedule of fixed assets.

⁹⁵ Reference: CDSL/A,I&C/DP/POLCY/2023/276 dated May 04, 2023



10. Nature and value of security against which the loan is secured is not provided under the balance sheet/ schedules to the balance sheet.
11. Related party disclosure is not given under notes to accounts. The Receivables from Group companies, Investment in Group companies/ associated company, Receivables from Directors, Loans & advances to Group companies/Directors of the company etc. should be included and considered for deductions. For such receivables, the full amount is not deducted for computation of net worth portion.
12. In case of related party transactions disclosure made by the auditors, the outstanding balance as on 31st March is not mentioned in the financial report.
13. Bifurcation of sundry debtors into more than and less than six months is not given under the schedule of current assets.
14. 50% of statutory contingent liability is not deducted from the net worth. The statutory contingent liability includes liability pertaining to GST, income tax, other statutory dues etc. which is under dispute.
15. The following items though not required to be deducted, are deducted for net worth computation:
 - a. Deposits with the exchanges
 - b. Bank Guarantee

10.6.3 Clarifications on certain items in the net worth certificate is given below:

Sr. No.	Particulars of net worth Computation	Clarifications
1.	Paid-up Capital + Free Reserves – Share Application Money (Total Reserves less Revaluation Reserves and Specified Reserves)	a) If the preference share capital is redeemable by end of the next financial year, it should be deducted from the net worth, unless the sufficient Capital Redemption reserve is created for redemption purpose. b) If the redeemable preference shares are part of the paid-up capital, the auditors should specifically provide the terms of redemptions e.g. Date of redemption, amount of redemption, no. of shares redeemable etc. c) Capital reserve, revaluation reserve, statutory reserve or any other specific reserve should not be considered as free reserve.



Sr. No.	Particulars of net worth Computation	Clarifications
2.	Receivable from / Investments in / Loans and advances to group Companies	a) Group companies include partnership firm, affiliates, associates, related entities including directors and their relatives. b) Investments by the company (DP) as Share application/allotment money in the group companies should be deducted.

10.6.4 DPs are requested to submit the scanned/digitally signed copies of Net worth certificate and AFS through email on NWAFS@cdslindia.com

10.6.5 In the event of the networth of the DP falling below the required network, the DP shall forthwith intimate CDSL of the same and shall, if so required by CDSL furnish to CDSL a fresh network certificate computed as prescribed and duly certified by a Statutory Auditors. CDSL may thereupon take such action as it may deem fit and necessary under the Act, Regulations, Bye Laws or Agreement.

10.6.6 Where the DP is a Non-Banking Finance Company or a RTA, it should maintain the net worth specified in Regulation 35(a)(ix) and 35(a)(x) of the SEBI (Depositories & Participants) Regulations respectively.

10.7 Surveillance Obligation of DP⁹⁶

10.7.1 In order to further strengthen the Surveillance framework for the Securities Market, all DPs are hereby advised to put in place a surveillance framework.

10.7.2 **Obligation of Depository Participants to frame Surveillance Policy:** DPs shall frame a surveillance policy based on nature of DP business (i.e., Bank, Stockbroker, Custodian etc.), type of clients, number of demat accounts, number of transactions etc. and which shall, inter alia, cover the following:

- Generation of suitable surveillance alerts which may be guided by indicative themes (the list is inclusive and not exhaustive) given below (refer 10.7.4)
- Review and disposal of transactional alerts provided by CDSL (Transactional alerts provided by CDSL will be based on some thresholds. DPs may have their own different thresholds or own parameters to generate additional alerts of their own in point I above, so as to detect any suspicious transaction activity).

⁹⁶ Reference: CDSL/OPS/DP/SYSTM/2021/309 dated July 15, 2021



- iii. Disposal of alerts within 30 days from the date of alerts generated at DP end and alerts provided by CDSL.
- iv. Reporting to CDSL and other authorities as applicable, in case of any abnormal activity
- v. Documentation of reasons for delay, if any, in disposition of alerts.
- vi. Framework of appropriate actions that can be taken by the Participant as per obligations under Prevention of Money Laundering Act (PMLA)
- vii. Record maintenance for the period as stipulated under applicable statutes
- viii. The surveillance policy of the DPs shall be reviewed once in a year

10.7.3 The surveillance policy of the Participant shall be approved by its Board of Directors. In case, the DP is incorporated outside India, then the surveillance policy of the DP may be approved by a Committee constituted to oversee its Indian Operations.

10.7.4 **Obligation of DPs to generate additional surveillance alerts:** DPs are required to generate appropriate surveillance alerts at their end, to enable them to effectively monitor the transactions of their clients at their end as per the laid down surveillance policy. The indicative themes on which DPs may formulate their own alerts are as under. The DPs also needs to analyse patterns and trends with respect to different themes. DPs shall put in place system to generate these alerts and obtain the approval of its Board in its next meeting.

Sr. No.	Indicative themes:
1	Alert for multiple demat accounts opened with same demographic details: Alert for accounts opened with same PAN /mobile number / email id/ bank account no. / address considering the existing demat accounts held with the DP.
2	Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
3	Frequent changes in details of demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.
4	Frequent Off-Market transfers by a client in a specified period
5	Off-market transfers not commensurate with the income/Networth of the client.
6	Pledge transactions not commensurate with the income/Networth of the client.
7	Off-market transfers (High Value) immediately after modification of details in demat account



Sr. No.	Indicative themes:
8	Review of reasons of off-market transfers provided by client for off-market transfers vis-à-vis profile of the client e.g. transfers with reason code Gifts with consideration, frequent transfers with reason code Gifts/Donation to unrelated parties, frequent transfers with reason code off-market sales
9	Alert for newly opened accounts wherein sudden Increase in transactions activities in short span of time and suddenly holding in demat account becomes zero or account becomes dormant after some time.
10	Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by their clients.

10.7.5 DPs should note that the above-mentioned alerts will be generated based on some threshold/parameters and are illustrative and not exhaustive. DPs have to analyze and review these alerts based on facts and verification of relevant documents including income/networth as provided by BO. Further, DPs are required to exercise their independent judgment and take appropriate action in order to detect any abnormal or suspicious transactions.

10.7.6 **Obligation of Depository Participants regarding Client due diligence:** The following activities required to be carried out by DPs for client due diligence:

- i. DPs are required to carry out the Due Diligence of their client(s) on an on-going basis.
- ii. DPs shall ensure that key KYC parameters of the clients are updated on a periodic basis as prescribed by SEBI and latest information of the client is updated in Depository System.

10.7.7 **Obligation of DPs for reporting the status of alerts generated by DPs**

- a. DPs are required to maintain register (electronic/physical) for recording of all alerts generated.
- b. While reviewing alerts, DP shall obtain transaction rationale, verify demat statement and also obtain supporting documents as required from the client
- c. After verifying the documentary evidences, DPs will record its observations for such identified transactions of its Client.
- d. With respect to the transactional alerts provided by Depository, DP shall ensure that all alerts are reviewed, and status thereof (Verified & Closed / Verified & Reported to Depository) including action taken is updated within 30 days. Detailed procedure w.r.t sharing of alert by CDSL with DPs and report submission by DPs in this regard will be provided separately.



- e. With respect to the alerts generated at the DP end, DP shall report instances with adverse observation, along with details of action taken, to CDSL within 7 days of the date of identification of adverse observation. Detailed procedure w.r.t reporting of alert by Participants will be provided separately

10.7.8 Obligation of Compliance officer and Internal Auditor/Concurrent Auditor of the DP

- a. The surveillance activities of DP shall be conducted under overall supervision of its Compliance Officer.
- b. A quarterly MIS shall be put up to the Board on the number of alerts pending at the beginning of the quarter, generated during the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with reasons for pendency and action plan for closure. Also, the Board shall be apprised of any exception noticed during the disposal of alerts.
- c. Internal auditor of DP shall review the surveillance policy, its implementation, effectiveness and review the alerts generated during the period of audit. Internal auditor shall record the observations with respect to the same in their report.
- d. Internal Auditor shall verify that the quarterly MIS is prepared and placed before the Board of the DP.

10.7.9 Obligation of Quarterly reporting of status of the alerts generated by DPs: DPs are also required to provide duly approved status of the alerts on a quarterly basis, in the following format to CDSL within 15 days from end of the quarter.

Status of Alerts generated by the DP:

Name of Alert	No. of alerts pending at the beginning of quarter	No. of new alerts generated in the quarter	No. of alerts Verified & closed in the quarter	No. of alerts reported to Depository	No. of alerts pending process at the end of quarter
----------------------	--	---	---	---	--

Details of any major surveillance action taken (other than alerts reported to Depository), if any, during the quarter:

Sr. No.	Brief action taken during the quarter
----------------	--



- 10.7.10 DPs who do not have anything to report, need to submit 'NIL Report' within 15 days from end of the quarter. Electronic Upload facility will be provided to DPs.
- 10.7.11 Penalty in case of late / non-submission of Quarterly Reporting of status:** In case of late / non-submission of quarterly report of the alerts generated by DP, as mentioned at Point B above, CDSL may levy penalty.
- 10.7.12 Disciplinary action for non-fulfilment of Surveillance obligation by DP:**
- i. DPs are advised to note that during CDSL inspection, if it is observed that the DP has not fulfilled their surveillance obligations, then appropriate disciplinary action shall be initiated against the DP.
 - ii. Any non-compliance with respect to surveillance obligations which may inter alia include delay in processing of alerts generated by DP / provided by CDSL and repeated instances of delay in reporting of the status of alerts, may result in further disciplinary action as deemed fit in terms of DP Operating instructions and Bye-laws of Depositories.
 - iii. It may further be noted that aforesaid measure does not preclude SEBI / Depository to take any further action(s), if the facts and circumstances so demand.
- 10.7.13 Compliance officer will be required to confirm compliance wrt Surveillance Policy to be framed by DPs by sending email to cdslalerts@cdslindia.com
- 10.7.14 DPs are advised to note the same and make necessary changes, in their back-office system.
- 10.7.15 CDSL has released a functionality whereby the surveillance related alerts related to Account Opening, Off-Market transfers, and Pledge/Unpledge/ Invocation generated by CDSL are made available to the respective DPs via Surveillance Portal and the DPs have to submit their response to the alerts via the said portal itself. Further, the DPs are required to submit count of the alerts generated by DPs on a quarterly basis, within 15 days from end of the quarter along with details of any major surveillance action taken (other than alerts reported to Depository), if any, during the quarter.



10.7.16 In this regard, DPs are advised to note following points once again.⁹⁷

1. Ensure that Quarterly reporting of Surveillance Alerts generated by DP will be reported on Surveillance Portal within 15 days from end of the quarter. DPs to ensure that alerts generated in demat accounts opened in Live connected branch will also be considered while reporting the count to CDSL.
2. It was also informed to the DPs that “With respect to the transactional alerts provided by Depository, DP shall ensure that all alerts are reviewed, and status thereof (Verified & Closed / Verified & Reported to Depository) including action taken is updated within 30 days”. Accordingly, DPs should ensure that all alerts provided by CDSL will be checked on regular basis by login to CDSL Surveillance Portal. DPs shall ensure that the Alerts are checked and compliance is submitted within 30 days.
3. DPs are also required to generate alerts based on the Alert theme indicators with the parameters set by the DP and post raising such alerts to BO, if DP finds any suspicious activities being carried out by BO, then such alerts must be reported to CDSL via ‘Adverse Observation Reporting’ tab under menu ‘Alert Reporting by DP’ of Surveillance portal.
4. DPs are required to exercise their independent judgment and take appropriate action to detect any abnormal or suspicious transactions. In addition to the above alerts, DPs are expected to generate additional alerts to detect and prevent any type of market manipulation activity carried out by their clients.

10.7.17 DPs are advised to refer to SEBI Circular no. SEBI/HO/ISD/ISD-PoD-2/P/CIR/2023/039 dated March 23, 2023 regarding Master Circular on Surveillance of Securities Market to ensure compliance.⁹⁸

10.8 Template for Supervisory Risk Assessment⁹⁹

10.8.1 DPs are advised to furnish the complete data of Template for Supervisory Risk Assessment inclusive of the data from their Live connected branches and submit the same to CDSL latest by EOD of Tuesday, January 03, 2023. In case of non-submission of Template for Supervisory Risk Assessment data by due date, the same will be reported to SEBI accordingly.

⁹⁷ Reference: CDSL/SURV/DP/ POLCY/2023/88 dated February 10, 2023

⁹⁸ Reference: CDSL/OPS/DP/POLCY/2023/189 March 24, 2023

⁹⁹ Reference: CDSL/OPS/DP/G ENRL/2022/731 December 27, 2022



10.8.2 DPs are required to furnish the data for financial year ended March 31, 2021, and March 31, 2022, in the google form link: - <https://forms.gle/Uh263VQbDJiJHNE7>. DPs will be able to access the same from Gmail id and will be able to access the same from google chrome.

10.8.3 DPs are directed to fill in the complete details and recheck the same before submission, since modifications will not be allowed once submitted. DPs will receive the response file after submission on the Gmail id from which the google form was submitted.

10.9 Opening of wholly owned subsidiaries or entering into joint ventures in other countries by the DPs¹⁰⁰

10.9.1 DPs are advised to take note of the format prescribed by SEBI for application for opening of Wholly Owned Subsidiaries or entering into Joint Ventures in other countries,

10.9.2 DPs are further advised to submit following documents along with request for NOC from CDSL for opening of Wholly Owned Subsidiaries or entering into Joint Ventures in other countries:

- a) Undertaking from the DP duly signed by the authorized signatory on the letter head of the company stating that pursuant to proposed setting up of wholly owned subsidiary or entering into joint ventures in other countries, we (name of the DP) shall undertake to maintain net worth required for DPs as prescribed and computed in the manner specified by CDSL.
- b) Information about the extent of liability of the DP with respect to the proposed setting up of wholly owned subsidiary or entering into joint ventures in other countries.

10.9.3 The abovementioned documents should be accompanied by necessary fees, as prescribed by CDSL from time to time.

10.9.4 DPs are advised to refer to SEBI Circular no. SEBI/HO/MIRSD/DoR/P/CIR/2022/61 dated May 13, 2022, regarding Guidelines for seeking NOC by Stock brokers / Clearing Members for setting up wholly owned subsidiaries, step down subsidiaries, joint ventures in GIFT IFSC¹⁰¹

¹⁰⁰ Reference: CDSL/OPS/DP/2258 dated January 17, 2011 and CDSL/A,I &C/DP/GENRL/2350 dated March 10, 2011

¹⁰¹ Reference: CDSL/OPS/DP/POLCY/2022/263 dated May 16, 2022



10.10 **Change in DP's shareholding pattern with change in control**¹⁰²

10.10.1 DPs are advised to take note of SEBI circular no. SEBI/HO/MIRSD/ MIRSD-PoD-2/P/CIR/2022/163 dated November 28, 2022, regarding Procedure for seeking prior approval for change in control.

10.10.2 To streamline the process of providing approval to the proposed change in control of intermediary, it has been decided as under:

- i. The Intermediary shall make an online application to SEBI for prior approval through the SEBI Intermediary Portal ('SI Portal') (<https://siportal.sebi.gov.in>).
- ii. The online application in SI portal shall be accompanied by the following information/declaration/undertaking about itself, the acquirer(s)/the person(s) who shall have the control and the directors/partners of the acquirer(s)/ the person(s) who shall have the control:
 - a. Current and proposed shareholding pattern of the applicant
 - b. Whether any application was made in the past to SEBI seeking registration in any capacity but was not granted? If yes, details thereof.
 - c. Whether any action has been initiated / taken under Securities Contracts (Regulation) Act, 1956 (SCRA)/Securities and Exchange Board of India Act, 1992 (SEBI Act) or rules and regulations made thereunder? If yes, the status thereof along with the corrective action taken to avoid such violations in the future. The acquirer/ the person who shall have the control shall also confirm that it shall honour all past liabilities / obligations of the applicant, if any.
 - d. Whether any investor complaint is pending? If yes, steps taken and confirmation that the acquirer/ the person who shall have the control shall resolve the same.
 - e. Details of litigation(s), if any.
 - f. Confirmation that all the fees due to SEBI have been paid.
 - g. Declaration cum undertaking of the applicant and the acquirer/ the person who shall have the control, duly stamped and signed by their authorized signatories that:
 - i. there will not be any change in the Board of Directors of incumbent, till the time prior approval is granted;
 - ii. pursuant to grant of prior approval by SEBI, the incumbent shall inform all the existing investors/ clients about the proposed change prior to effecting

¹⁰² Reference: CDSL/OPS/DP/POLCY/2022/694 dated December 06, 2022



the same, in order to enable them to take informed decision regarding their continuance or otherwise with the new management; and

iii. the 'fit and proper person' criteria as specified in Schedule II of SEBI (Intermediaries) Regulations, 2008 are complied with.

h. In case the incumbent is a registered stock broker, clearing member, depository participant, in addition to the above, it shall obtain approval /NOC from all the stock exchanges/clearing corporations/depositories, where the incumbent is a member/depository participant and submit self-attested copy of the same to SEBI.

iii. The prior approval granted by SEBI shall be valid for a period of six months from the date of such approval within which the applicant shall file application for fresh registration pursuant to change in control.

10.10.3 To streamline the process of providing approval to the proposed change in control of an intermediary in matters which involve scheme(s) of arrangement which needs sanction of the National Company Law Tribunal ("NCLT") in terms of the provisions of the Companies Act, 2013, the following has been decided:

- i. The application seeking approval for the proposed change in control of the intermediary shall be filed with SEBI prior to filing the application with NCLT.
- ii. Upon being satisfied with compliance of the applicable regulatory requirements, an in-principle approval will be granted by SEBI;
- iii. The validity of such in-principle approval shall be three months from the date issuance, within which the relevant application shall be made to NCLT.
- iv. Within 15 days from the date of order of NCLT, the intermediary shall submit an online application in terms of paragraph 3 of this circular along with the following documents to SEBI for final approval:
 - a. Copy of the NCLT Order approving the scheme;
 - b. Copy of the approved scheme;
 - c. Statement explaining modifications, if any, in the approved scheme vis-à-vis the draft scheme and the reasons for the same; and
 - d. Details of compliance with the conditions/ observations, if any, mentioned in the in-principle approval provided by SEBI.



INFORMATION/ DOCUMENTS TO BE SUBMITTED TO CDSL

Sr. No.	Particulars	Periodicity for submission of reports	Due dates for receipt by CDSL	Mode of submission
1.	BO Grievances Report	Monthly	10 th of the following month	Online Submission
2.	Internal Audit Reports (IAR) and Concurrent Audit Report (CAR) of risk prone areas	Half yearly	15 th May for half year ended 31 st March & 15 th November for half year ended 30 th September	Online Submission
3.	Audited Net Worth Certificate	Yearly	30 th September, after end of financial year	Hard copy duly certified by the statutory auditor in the format as specified by CDSL. DPs are requested to submit the scan/digitally signed copies of Networth as of 31 st March via email to the designated email id
4.	Audited Financial Statements	Yearly	30 th September, after end of financial year	Hard copy duly certified by the statutory auditor in the format as specified by CDSL DP's are requested to submit the scan/digitally signed copies of AFS as of 31 st March via email to the designated email id
5.	Submission/ Dissemination of DP Tariff/ Charges structure	Yearly	On or before 30 th April every year and as and when tariff structure is revised	Data on tariff structure to be uploaded on CDSL website. No need to submit the hardcopy of the tariff to CDSL which is uploaded by them through their DP easiest login



Sr. No.	Particulars	Periodicity for submission of reports	Due dates for receipt by CDSL	Mode of submission
6.	Compliance Officer Details	If new officer appointed or any change in the compliance officer	Immediately	Hard copy in the format as specified by CDSL in the Operating Instructions
7.	Compliance Certificate	Half yearly	Before 31 st July for the half year period from January to June & 31 st January for the half year period from July to December	Online submission of digitally signed certificate on CDSL
8.	Information in Risk Assessment Template	Half Yearly	Before 31 st October for the half year period from April to September & 30 th April for the half year period from October to March	Online submission of Risk Assessment Template through web-CDAS
10.	Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems ¹⁰³	Quarterly	15 days after the end of the quarter	Online submission of Cyber Security & Cyber Resilience framework on audit web portal of CDSL
11.	Number of Suspicious Transaction Report (STR) filed directly with FIU-IND	Monthly	Within 7 days of the following month (Nil report need not be submitted)	Soft copy in prescribed format to pmla@cdslindia.com



Sr. No.	Particulars	Periodicity for submission of reports	Due dates for receipt by CDSL	Mode of submission
	during the a given month			
12.	Status of the Surveillance alerts generated by DPs	Quarterly	within 15 days from end of the quarter	Online Submission
13.	Reporting of Cyber-attacks, threats (CYBER INCIDENT REPORT) ¹⁰³	Immediately on occurrence of the incident	Immediately on occurrence of the incident	Through email to the designated email id
14.	Reporting of Cyber-attacks, threats ¹⁰³ (Cyber Incident Report)	Quarterly	15 days after expiry of the quarter	Online Submission
15.	System Audit Report (Cyber Security Annual Report) ¹⁰³	Annually	3 months from the end of Financial year	Online Submission
16.	VAPT	Annually	Within one month of completion of VAPT	Online Submission
17.	Compliance of closure of findings identified during VAPT	As and when	Within three months post the submission of final VAPT report	Online Submission

¹⁰³ Reference: CDSL/AUDIT/DP/POLCY/2021/302 dated July 9, 2021



Sr. No.	Particulars	Periodicity for submission of reports	Due dates for receipt by CDSL	Mode of submission
18.	DIS Scanning & upload	Daily	After execution - By the end of next working day	Online on webCDAS
19.	Roadmap (including details of major activities, timelines, etc.) for the implementation of the framework wrt cloud services	One time	Within three months of issuance of framework	In format prescribed by CDSL
20.	Quarterly progress report as per the roadmap submitted by the RE	Quarterly	From three to twelve months of issuance of framework	In format prescribed by CDSL
21.	Compliance with respect to the cloud services framework	Ongoing basis	Regularly	In format prescribed by CDSL

INFORMATION/ DOCUMENTS TO BE SUBMITTED TO CDSL

Sr. No.	Compliance Reports
22.	Compliance report in respect of Inspection / Internal Audit / Concurrent Audit, duly counter signed by concurrent / internal auditor should be submitted to CDSL within 30 days from receipt of non-compliance letter from CDSL.



INFORMATION/ DOCUMENTS TO BE SUBMITTED TO FIU-IND

Sr. No.	Particulars	Periodicity for submission of reports	Due dates for receipt by CDSL	Mode of submission
23.	Suspicious Transaction Report (STR)	Fortnightly -on receiving alerts from CDSL or whenever alerts are generated by DP or whenever suspicious transactions are noticed by DPs	To be submitted within 7 days of discovering the suspicious transaction to FIU-IND, New Delhi	Online Submission



Chapter 11 : Grievance Redressal

11.1 Grievance Redressal

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional guidelines with respect to Grievance Redressal shall require to be complied with:

- 11.1.1 The DPs are advised to designate an exclusive Email Id of the Grievance Redressal Department or Compliance Officer for the purpose of registering complaints of investors and for taking necessary follow-up actions. This exclusive email ID should be prominently displayed on the DP's website and in the various materials / pamphlets / advertisement campaigns initiated by the DP for creating investor awareness.¹⁰⁴
- 11.1.2 CDSL has provided online facility to DPs for upload/download of Investor Grievance related correspondence through electronic mode. DP would be able to access Investor Grievance module through electronic mode platform. Scanned copies of replies / responses for BO Grievances need to be uploaded by DP through electronic mode. DPs are advised to monitor the portal of online grievance redressal correspondence on daily basis and resolve the grievance of the BO within stipulated time frame.¹⁰⁵

11.2 Display of grievance redressal mechanism¹⁰⁶

- 11.2.1 DPs shall prominently display in their office basic information about the grievance redressal mechanism available to investors.

11.3 Grievance Redressal through SCORES¹⁰⁷

- 11.3.1 The investor grievances received by SEBI against DPs will be taken up electronically with the concerned Depositories through SCORES (<https://scores.gov.in/Admin>). The Depositories shall, in turn, take up the matter with the concerned DPs. The DPs shall take adequate steps for redressal of grievances within one month from the date of receipt of the complaint and keep the investor/Depositories duly informed of the action taken thereon. Failure to comply with the said requirement will render the DP liable for penal action.

¹⁰⁴ Reference: CDSL/OPS/DP/816 dated January 03, 2007

¹⁰⁵ Reference: CDSL/AI&C/DP/POLCY/2020/163 dated March 30, 2020

¹⁰⁶ Reference: CDSL/OPS/DP/POLCY/4675 dated September 02, 2014

¹⁰⁷ Reference: CDSL/OPS/DP/POLCY/2635 dated September 15, 2011



- 11.3.2 DP should provide a link to SCORES portal, within the demat account dashboard of clients to make it easier to lodge grievances. Further, DP shall display the following information on their website to make the complaint redressal mechanism through SCORES more efficient.¹⁰⁸

Filing compliant on SCORES – Easy & quick

- a. Register on SCORES portal
- b. Mandatory details for filing complaints on SCORES
 - i. Name, PAN, Address, Mobile Number, E-mail ID
- c. Benefits:
 - i. Effective Communication
 - ii. Speedy redressal of the grievances

Further, DPs are advised to include procedure for filing of complaints on SCORES and benefits for the same in the welcome kit which is being provided to the investors at the time of account opening

11.4 Investor Charter

- 11.4.1 DPs are advised to bring the Investor Charter and its linked contents, to the notice of their clients (existing as well as new clients) through disclosing the Investor Charter on their respective websites and also, to make the investor charter available at prominent places in their office, provide a copy of Investor Charter as a part of account opening kit to the clients, through e-mails/letters etc.¹⁰⁹
- 11.4.2 DPs may note that on verification of the said compliance it has been observed that there is no uniformity in complying with the said circular by the DPs. Further the link to the Investor Charter published is not easily accessible and the Investor Charter is not published in true letter and spirit. In some cases, it is observed that the DPs have published the charter with SEBI name and emblem and not having any connect to the respective DP. DPs are once again advised to review the above and ensure that the Disclosure of the Investor Charter is displayed on their website with proper link in their homepage under the respective DP name. DPs are requested to take note of the same and ensure compliance and confirm the same by providing the details of the link where the Investor Charter is published through email addressed to audit@cdslindia.com with subject head as “Investor Charter and DP ID and DP Name”.¹¹⁰

¹⁰⁸ Reference: CDSL/OPS/DP/POLCY/2018/132 dated March 16, 2018 and CDSL/OPS/DP/POLCY/2019/332 dated July 04, 2019

¹⁰⁹ Reference: CDSL/OPS/DP/POLCY/2021/589 dated December 25, 2021

¹¹⁰ Reference: CDSL/A,I&C/DP/POLCY/2022/319 dated June 07, 2022



11.5 Disclosure of the complaints received against DPs

11.5.1 To bring about transparency in the Investor Grievance Redressal Mechanism, SEBI has decided that all the DPs shall disclose on their respective websites, the data on complaints received against them or against issues dealt by them and redressal thereof, latest by 7th of the succeeding month, as per the prescribed format. These disclosure requirements are in addition to existing mandatory requirements.¹¹¹

11.6 Investor Grievances escalation matrix¹¹²

11.6.1 To further strengthen the process of handling Investors Grievances, DPs are advised to take the below measures:

- a. Multiple modes of communication should be made available to the investors, in order to ensure smooth process in filing the complaints.
- b. Employ qualified/trained and dedicated officials to beef up the complaint redressal mechanism for better handling and suitable closures.
- c. Investor Grievances escalation matrix to be explicitly displayed on the DP website under the 'Contact Us' page. The 'Contact Us' link should be placed on the index/homepage of the website. Upon clicking the same, it should display the requisite details.
- d. Escalation matrix should also be a part of the complaint redressal communications between the DPs and Investors.
- e. Acknowledgment should be sent to the investor on receipt of grievance and should state the Complaint reference number in it. This will reduce registering of duplicate complaints.
- f. DPs, who are also a Stockbrokers, shall provide separate escalation matrix for Broking related queries. In case they have a common grievance handling unit, they may display the common Escalation matrix as stated under point 'c'.
- g. Enhance Investor education vide educational videos, webinars, flyers, bulletin, etc.
- h. Regular updates should be provided to investors on changes in rules/regulations through support portals/ email.
- i. Details of services provided by DP/ Depository to clients may be displayed on homepage of the website.
- j. Provision shall be made for online submission and acceptance of requests such as changes in demographic details, closure & KYC related matters.
- k. Conduct regular system audits to reduce the occurrence of technical issues and downtimes.

¹¹¹ Reference: CDSL/OPS/DP/POLCY/2021/589 dated December 25, 2021

¹¹² Reference: CDSL/IG/DP/2022/468 dated August 17, 2022 and CDSL/IG/DP/2022/653 dated November 10, 2022



11.6.2 DPs are advised to comply with the following:

- a. Contact numbers mentioned for each escalation level should be different.
- b. Contact number provided should be handled by escalated person and not by IVRS
- c. In case contact number is handled by IVRS, it should allow the caller/complainant to reach the desired escalated person.
- d. Escalated person's number provided should be valid /correct
- e. In addition to the above, DPs are also advised to include working hours of each escalation level (e.g., Monday to Saturday 9.00 am to 12.30 pm and 2.00 pm to 6.00 pm.).

11.7 Master Circular on the redressal of investor grievances through the SEBI Complaints Redress System (SCORES) platform¹¹³

11.7.1 DPs are advised to refer to SEBI Circular no. SEBI/HO/OIAE/IGRD/P/CIR/2022/0150 dated November 07, 2022, regarding Master Circular on the redressal of investor grievances through the SEBI Complaints Redress System (SCORES) platform for necessary compliance.

¹¹³ Reference: CDSL/OPS/DP/POLCY/2022/650 dated November 9, 2022



Chapter 12 : Maintenance of Website by DP

12.1 Maintenance of a website by depository participants¹¹⁴

12.1.1 SEBI, through various circulars, has mandated certain information to be published by depository participants (DP) on their respective websites.

12.1.2 A designated website brings in transparency and helps the investors to keep themselves well informed about the various activities of the DP. In view of the same, considering the advancement in technology and need to provide better services to the investors, all DPs are mandated to maintain a designated website.

12.1.3 Such website shall mandatorily display the following information, in addition to all such information, which have been mandated by SEBI/stock exchanges/depositories from time to time.

- I. Basic details of the DP such as registration number, registered address of Head Office and branches, if any.
- II. Names and contact details such as email ids etc. of all key managerial personnel (KMPs) including compliance officer.
- III. Step-by-step procedures for opening an account, filing a complaint on a designated email id, and finding out the status of the complaint, etc.

The URL to the website of a DP shall be reported to the depositories. Any modification in the URL shall be reported to depositories within 3 days of such changes.

¹¹⁴Reference: CDSL/OPS/DP/POLCY/2023/113 dated February 17, 2023



Chapter 13 : DP Branches/Service Centres

13.1 DP Branch/ DP Service Centre¹¹⁵

In addition to the procedure already specified in the Operating Instructions, the Bye Laws, the following additional points have to be complied with on set up of the DP:

1. The branches of the DP must have the requisite hardware/software as prescribed by CDSL.
2. The branch premises must be owned/leased or licensed to the main DP.
3. The branch of the DP must have the communication network registered in the name of the main DP or leased or licensed to the main DP.
4. The branches of the DP must have adequate provisions for safety and security of the documents pertaining to the BOs.
5. The main DP should submit an undertaking to fulfill all rights and obligations on behalf of all its branches.
6. DPs shall through their easiest login able to add new service centres; modify existing details or delete the existing service centre records.

13.2 Outsourcing of activities by DPs¹¹⁶

13.2.1 DPs are advised to comply with the guidelines issued by SEBI vide circular no. CIR/MIRSD/24/2011 Dated December 15, 2011 regarding outsourcing of activities related to services offered by intermediaries.

13.2.2 The principles for outsourcing by intermediaries have been framed, which shall be followed by all intermediaries registered with SEBI.

13.2.3 The intermediaries desirous of outsourcing their activities shall not, however, outsource their core business activities and compliance functions.

13.2.4 Regarding Know Your Client (KYC) requirements, the intermediaries shall comply with the provisions of SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011 and Guidelines issued thereunder from time to time.

The intermediaries shall be responsible for reporting of any suspicious transactions / reports to FIU or any other competent authority in respect of activities carried out by the third parties.

¹¹⁵ Reference: CDS/OPS/DP/75(A) dated January 22, 2001 and CDSL/ADM/DP/GENRL/6272 dated December 02, 2016

¹¹⁶ Reference: CDSL/OPS/DP/POLCY/2775 dated December 27, 2011



Chapter 14 : Prevention of Money Laundering Act, 2002 (PMLA)

14.1 Guidelines to DPs on PMLA¹¹⁷

14.1.1 DPs are advised to refer SEBI Circular no. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023, regarding 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.

14.1.2 The DPs should adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following four specific parameters which are related to the overall 'Client Due Diligence Process':

- i. Policy for acceptance of clients;
- ii. Procedure for identifying the clients;
- iii. Risk Management;
- iv. Monitoring of Transactions.

14.1.3 SEBI/CDSL has from time to time issued circulars/directives with regard to Know Your Client (KYC), Client Due Diligence (CDD), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) specifying the minimum requirements. It is emphasized that the DPs may, according to their requirements, specify additional disclosures to be made by clients to address concerns of money laundering and suspicious transactions undertaken by clients.

14.1.4 A DP should adhere to the following aspects spelt out in the guidelines regarding PMLA:

- a. Essential Principles
- b. Obligation to establish policies and procedures
- c. Written Anti Money Laundering Procedures
- d. Client Due Diligence (CDD)
- e. Policy for acceptance of clients
- f. Client identification procedure
- g. Reliance on third party for carrying out Client Due Diligence (CDD)
- h. Risk Management, including Risk-based Approach and Risk Assessment
- i. Monitoring of Transactions
- j. Suspicious Transaction Monitoring and Reporting

¹¹⁷ Reference: CDSL/OPS/DP/POLCY/2023/185 dated March 23, 2023



- k. Record Management, including Information to be maintained, Record Keeping and Retention of Records
- l. Procedure for freezing of funds, financial assets or economic resources or related services
- m. List of Designated Individuals/Entities
- n. Jurisdictions that do not or insufficiently apply the FATF Recommendations
- o. Reporting to Financial Intelligence Unit-India
- p. Designation of officers for ensuring compliance with provisions of PMLA
- q. Hiring and Training of Employees and / Investor Education

14.1.5 DPs shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the DP.

14.1.6 DPs should send a copy of the Policy directly to FIU-IND.¹¹⁸

14.2 Commonly observed discrepancies in inspection of DPs in the area of PMLA requirements¹¹⁹

14.2.1 During the inspection of the DPs by CDSL and SEBI, certain non-compliances have been observed in the area of implementation of above referred SEBI circular which may expose DPs to potential risk. In order to raise the compliance level and to mitigate the risk, DPs are advised to ensure that following steps are taken:

1. Anti-Money Laundering policy is framed as per SEBI guidelines and revised periodically.
2. The information on Financial Status/income details of clients is obtained at the time of opening of demat account. Subsequently, it should be periodically updated in CDAS/back office. The DP has to satisfy that the transactions carried out by the client are commensurate with his income. If any abnormality is noticed, DP should file STR.
3. Designated Director is appointed as per SEBI guidelines.
4. Parameters for risk categorization of clients are provided in the AML policy.
5. Independent verification of clients undertaken during client acceptance is indicated in the policy.
6. Categorization of clients into “Clients of Special Category” (CSC) is done by the DP.

¹¹⁸ Reference: CDSL/OPS/DP/793 dated November 21, 2006

¹¹⁹ Reference: CDSL/A,I&C/DP/POLCY/4690 dated September 08, 2014



7. To conduct ongoing training programme for employees so that DP staff are adequately trained in AML and CFT (Combating Financing of terrorism) procedures.
8. The DP has systems in place for continuous monitoring of transactions vis-à-vis income of the client. Alerts sent by CDSL are monitored and a suspicious transaction register is maintained.
9. Policy on Employees hiring/training and investor education included in PMLA policy.

14.3 Appointment of a Principal Officer¹²⁰

- 14.3.1 To ensure that the DPs properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors.
- 14.3.2 Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU-IND. As a matter of principle, it is advisable that the 'Principal Officer' is of a sufficiently senior position and is able to discharge the functions with independence and authority.

14.4 Appointment of a Designated Director¹²¹

- 14.4.1 The DPs shall designate a person as a 'Designated Director'.
- 14.4.2 In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under:

“Designated director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes –

 - a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,
 - b) the managing partner if the reporting entity is a partnership firm,
 - c) the proprietor if the reporting entity is a proprietorship firm,
 - d) the managing trustee if the reporting entity is a trust,

¹²⁰ Reference: CDSL/OPS/DP/POLCY/2023/185 dated March 23, 2023

¹²¹ Reference: CDSL/OPS/DP/POLCY/2023/185 dated March 23, 2023



- e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
- f) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above”.

14.4.3 In terms of Section 13 (2) of the PMLA, the Director, FIU – IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the DP with any of its AML/CFT obligations.

14.4.4 DP shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND

14.5 Reporting of potentially Suspicious Transactions¹²²

14.5.1 For the purpose of reporting the details of suspicious transactions to the FIU-IND, CDSL has evolved certain criteria for generating alerts for DPs containing details of transactions that are potentially suspicious. CDSL will send alerts to DPs. Such alerts may enable DPs to identify suspicious transactions.

14.5.2 DPs will be required to analyze and ascertain whether the transactions intimated by CDSL are suspicious in nature. For this purpose, DPs are advised to evolve their own procedure for scrutiny of the alerts for identifying suspicious transactions, so as to comply with the provisions of the PMLA and rules and guidelines thereof issued by FIU-IND/ SEBI from time to time.

14.5.3 DPs should note that they should not restrict themselves to scrutinizing the transactions appearing in the alerts given by CDSL and should evolve their own mechanism to monitor all transactions.

14.5.4 If DPs identify any transaction as suspicious in nature, they should submit the report directly to the Director, FIU-IND, New Delhi, in the prescribed format within 7 working days of establishment of suspicion.

14.5.5 DPs are also required to maintain a Register where they should note the action taken on such report.

¹²² Reference: CDSL/OPS/DP/762 dated October 06, 2006



- 14.5.6 The DPs are advised to note that CDSL's DP Operating Instructions and various communiqués issued, clearly outline the documents required to be obtained for account opening. However, DPs are required to exercise due diligence while establishing the identity of the intending BO(s), thus ensuring the safety and integrity of the depository system, as the provisions of PMLA stipulates that the DPs are also required to be aware of the nature of business and financial status of the intending BO(s) at the time of account opening or executing any transactions thereafter.
- 14.5.7 DPs are advised to refer email sent to the Designated Director & Principal Officer on 28-Jul-2022 and 07-Dec-2022, informing about the Supplemental Guidelines for detecting suspicious transactions under rule 7(3) of Prevention of Money Laundering (Maintenance of Records) Rules, 2005, issued by FIU-IND.
- 14.5.8 DPs are advised to note that the reports from the month of December 2022, onwards have been provided on surveillance application of CDSL. (CDAS – Surveillance Application – Inquiry – FIU Inquiry) & (CDAS – Surveillance Application – Download – FIU Report Download).
- 14.5.9 DPs are advised to ensure that necessary access rights are provided to concerned officials. Designated Directors & Principal Officers are advised to ensure that all the alerts provided are downloaded on periodic basis, thoroughly analyzed, processed and necessary actions are taken.¹²³
- 14.5.10 The DPs should submit the report to FIU- IND in the format developed under the FINnet PROJECT.¹²⁴
- 14.5.11 DPs are informed that that FIU-IND has advised that STRs shall not be accepted through FINnet gateway without digital signature.¹²⁵
- 14.5.12 DPs are advised to carefully analyze alerts sent by CDSL and file STRs with FIU-IND in appropriate cases. Further, DP should provide the following information in the grounds of suspicion so that FIU-IND will be in a position to analyze STRs correctly.¹²⁶
1. Details of initial alert sent by CDSL
 2. Information collected during analysis of alert
 3. KYC information of the client

¹²³ Reference: CDSL/PMLA/DP/POLCY/2023/184 dated March 23, 2023

¹²⁴ Reference: CDSL/OPS/DP/POLCY/3252 dated September 29, 2012

¹²⁵ Reference: CDSL/OPS/DP/POLCY/5815 dated March 15, 2016

¹²⁶ Reference: CDSL/OPS/DP/1448 dated January 29, 2009



4. Period of the activities being reported
5. Quantum of the activities being reported
6. ISIN/Issuer Name, if reported transaction relates to a particular ISIN/ Issuer
7. Explanation regarding the reported suspicion

14.6 Registration of the Reporting Entities (REs) in FINnet 2.0 system

- 14.6.1 FIU-IND vide its communication dated May 23, 2022, has informed the depository about the fresh registration of the Reporting Entities (REs) in FINnet 2.0 system from 19.01.2022 and requested to take up the matter with all the registered Depository Participants for registration in FINnet 2.0 system.
- 14.6.2 Depository Participants are Reporting Entities to FIU-INDIA as defined under Section 2(wa) read with Section 2(n) of the PMLA.
- 14.6.3 As part of the envisaged, FINnet 2.0 system all Reporting Entities (REs) registered in FINnet 1.0 are required to re-register themselves in FINnet 2.0 module. Further, it may be noted that as part of the re-registration exercise REs are required to register Principal Officer as well as Designated Director by providing the necessary details.¹²⁷
- 14.6.4 DPs are advised to get registered on FINnet 2.0 Mandatorily without fail, otherwise it will be treated as non-compliance with the Reporting Entity's obligations under PMLA.
- 14.6.5 DPs are requested to complete registration in FINnet 2.0 system immediately and confirm by sending an email to pmla@cdslindia.com from email ID of Principal Officer / Designated Director with subject line as <DP ID> registration done on FINnet 2.0¹²⁸
- 14.6.6 DPs are advised to refer Advisory Notifications for Registration of Reporting Entity in multiple categories and Reporting of Registered/Mandate accounts to all the reporting entities circulated by FIU IND.¹²⁹

¹²⁷ Reference: CDSL/OPS/DP/POLCY/2022/288 dated May 27, 2022

¹²⁸ Reference: CDSL/PMLA/DP/POLCY/2022/648 dated November 09, 2022

¹²⁹ Reference: CDSL/OPS/DP/POLCY/5521 dated October 27, 2015



14.7 List of Designated Individuals/ Entities¹³⁰

14.7.1 The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. DPs shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by SEBI from time to time shall be taken note of for compliance.

14.7.2 An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at <https://press.un.org/en/content/press-release>. The details of the lists are as under:

- i. The “ISIL (Da’esh) & Al-Qaida Sanctions List”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at: <https://www.un.org/securitycouncil/sanctions/1267/press-releases>.
- ii. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases.

14.7.3 DPs are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. DPs shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

14.7.4 DPs shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

14.7.5 DPs shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.

¹³⁰ Reference: CDSL/OPS/DP/POLCY/2023/185 dated March 23, 2023



14.7.5 Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in. DPs shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, “G” Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

14.8 Jurisdictions that do not or insufficiently apply the FATF Recommendations¹³¹

14.8.1 FATF Secretariat after conclusion of each of its plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by the registered intermediaries.

14.8.2 The DPs shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the DPs are not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

14.8.3 As directed by SEBI to Depositories, a written confirmation as per Template is required from the DP confirming that the actions required are taken and complied with.

Actions may include:

1. By carrying out appropriate due- diligence on existing clients.
2. Making sure that appropriate alert mechanisms have been put in place to identify the business relationships and transactions with the said jurisdictions.
3. Any other measures necessary to effectively implement the action required.

¹³¹ Reference: CDSL/OPS/DP/POLCY/2023/185 dated March 23, 2023



14.8.4 In view of the above, DPs are mandatorily required to furnish the information to CDSL as per the prescribed procedure.¹³²

14.9 Amendments to PMLA Rules

14.9.1 DPs are advised to refer Amendments to Prevention of Money-laundering (Maintenance of Records) Rules, 2005 for necessary compliance.¹³³

¹³² Reference: CDSL/OPS/DP/POLCY/2022/175 dated March 29, 2022

¹³³ Reference: CDSL/OPS/DP/1847 dated January 06, 2010 and CDSL/OPS/DP/POLCY/2018/294 dated June 07, 2018



Chapter 15 : Cyber Security and Cyber Resilience Framework

15.1 Cyber Security & Cyber Resilience Framework for DPs

15.1.1 SEBI vide its circular no. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 has issued a Cyber Security and Cyber Resilience Framework for Depository Participants. DPs should take note of the contents of the aforesaid SEBI circular and should have robust cyber security and cyber resilience framework to protect the integrity of data and essential facilities and perform systemically critical functions without breach of privacy.

15.1.2 DPs should formulate a comprehensive Cyber Security and Cyber Resilience policy document approved by its Board / Partners / Proprietor, and should be reviewed at least annually.

Quarterly reports containing information on cyber-attacks and threats experienced by Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats should be submitted to Depositories.

15.1.3 DPs should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.

15.1.4 DPs shall arrange to have their systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA/CISM qualified auditor to check compliance with the aforesaid SEBI circular and shall submit the report to Depositories along with the comments of the Board / Partners / Proprietor of DP within three months of the end of the financial year.¹³⁴

15.1.5 DPs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The Board/Partners/Proprietor of the DPs shall approve the list of critical systems. To this end, DPs 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.¹³⁵

¹³⁴ Reference : CDSL/OPS/DP/POLCY/2018/641 dated December 04, 2018

¹³⁵ Reference : CDSL/OPS/DP/POLCY/2022/323 dated June 09, 2022



15.2 Submission of Cyber Incident by DPs

15.2.1 All Cyber-attacks, threats, cyber-incidents and breaches experienced by DPs shall be reported to Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. The details of such incidents should be submitted to dpinfosec@cdslindia.com.¹³⁶

15.2.2 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 DPs, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.¹³⁷

15.2.3 DPs are required to make online submissions in prescribed format to CDSL on Quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by DPs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other DPs/ Depositories and SEBI.¹³⁸

15.2.4 The time period for submission of the report shall be 15 days after the end of the quarter.¹³⁹

The above information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.

15.3 Comprehensive Cyber Audit to check the compliance of Cyber Security and Cyber Resilience provisions

15.3.1 Auditors qualified in following certifications can audit the systems DPs to check the compliance of Cyber Security and Cyber Resilience provisions:

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)).

¹³⁶Reference: CDSL/OPS/DP/POLCY/2022/374 dated July 01, 2022, CDSL/OPS/DP/POLCY/2022/420 dated July 26, 2022 & CDSL/AUDIT/DP/POLCY/2021/302 dated July 9, 2021

¹³⁷Reference: CDSL/OPS/DP/POLCY/2022/374 dated July 01, 2022

¹³⁸Reference: CDSL/OPS/DP/POLCY/2022/374 dated July 01, 2022, CDSL/OPS/DP/POLCY/2019/535 dated October 23, 2019, CDSL/OPS/DP/POLCY/2022/420 dated July 26, 2022 & CDSL/AUDIT/DP/POLCY/2021/302 dated July 9, 2021

¹³⁹Reference: CDSL/OPS/DP/POLCY/2019/535 dated October 23, 2019 and CDSL/OPS/DP/POLCY/2022/374 dated July 01, 2022



The periodicity of audit for the purpose of compliance with Cyber Security and Cyber Resilience provisions for depository participants shall be annual.¹⁴⁰

15.3.2 DPs shall submit with Depository a declaration from the MD/CEO/Partners/ Proprietors certifying compliance by the DPs with all SEBI Circulars and advisories related to Cyber security from time to time, along with the Cyber audit report.¹⁴¹

15.4 Standard Operating Procedures (SOP) for handling Cyber Security Incidents¹⁴²

15.4.1 DPs are advised to formulate and adhere with the SOP for handling and reporting of Cyber Security Incidents.

15.4.2 The following aspects shall form part of the SOP which needs to be complied with by DPs:

- DPs shall have documented Cyber Security incident handling process document i.e., Standard Operating Procedure (SOP) in place.
- DPs shall examine the incidents and classify the incidents into High/Medium/Low as per their cyber security incident handling document.
- The cyber security incident handling document shall define Actions/Response Mechanisms for the incident based on severity.
- DPs shall report the incident to Indian Computer Emergency Response Team (CERT-In).
- DPs shall provide the reference details of the reported incident to the Depository and SEBI. DPs shall also provide details regarding whether CERT-In team is in touch with the DPs for any assistance on reported incident. If the incident is not reported to CERT-In, DPs shall submit the reasons for the same to the Depository and SEBI.
- DPs shall communicate with CERT-In/MHA/Cybercrime police for further assistance on the reported incident.
- DPs shall submit details on whether the incident has been registered as a complaint with law enforcement agencies such as Police or cyber security cell. If yes, details need to be provided to Depository and SEBI. If not, reason for not registering complaint should also be provided to Depository and SEBI.
- The details of reported incidents and submission to various agencies by the DPs shall also be submitted to Division Chiefs (in charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI.

¹⁴⁰ Reference: CDSL/OPS/DP/POLCY/2019/535 dated October 23, 2019

¹⁴¹ Reference: CDSL/OPS/DP/POLCY/2022/323 dated June 09, 2022

¹⁴² Reference: CDSL/OPS/DP/POLCY/2021/207 dated May 04, 2021



- The Designated Officer of the DPs shall continue to report any unusual activities and events within 24 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter.

15.5 Cyber Security - Information of Designated Officer¹⁴³

All DPs are required to designate a senior official or management personnel as Designated officer for the purpose of enforcing the SEBI circular on the framework for cyber security & cyber resilience for DPS.

DPs shall provide the information of the Designated Officer to CDSL.

15.6 Cyber Security Advisory¹⁴⁴

As financial services are a critical information infrastructure, it has been observed that it is one of the primary targets of cyber-attacks. To ensure continuous availability of services and to prevent cyber-attacks, all DPs are requested to ensure the following:

- Take review of the cyber security safeguards put in place, and any gaps found should be fixed on priority.
- Adequate safety and security measures (like intrusion detection/prevention system, anti-virus, firewall, etc.) are in place to protect the critical data, infrastructure, and applications.
- Review the communication links provisioned for trading, communications and other services exposed to the customers and partners on the internet / private networks. Ensure that all the internet links and services are adequately protected from cyber-attacks including DoS / DDoS attacks.
- Continuously monitor the applications and services for their availability and response time.
- Any cybersecurity incident is promptly reported to the relevant authorities including CDSL. Such incident should be reported to CDSL on dpinfosec@cdslindia.com and helpdesk@cdslindia.com.
- All Depository Participants are also advised to continue to adhere to cyber security guidelines / advisories issued by SEBI in the past and follow best industry practices and comply with other guidelines issued by CERT-In (<https://cert-in.org.in>) and NCIIPC (<https://www.nciipc.gov.in>) from time to time.

¹⁴³ Reference: CDSL/OPS/DP/POLCY/2021/210 dated May 06, 2021

¹⁴⁴ Reference : CDSL/OPS/DP/POLCY/2021/515 dated November 16, 2021



15.7 Vulnerability Assessment and Penetration Tests (VAPT)

15.7.1 DPs 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 DPs 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.

15.7.2 DPs shall conduct VAPT at least once in a financial year. All DPs are required to engage only CERT-In empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Depositories after approval from Technology Committee of DPs, within 1 month of completion of VAPT activity. In addition, DPs 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.

Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Depositories within 3 months post the submission of final VAPT report.¹⁴⁵

15.7.3 DPs are required to communicate the status of the implementation of the provisions of the SEBI Circular no. SEBI/HO/MIRSD/ TPD/P/CIR/2022/80 dated June 07, 2022 to CDSL within 10 days from the date of the Circular.¹⁴⁶

15.7.4 VAPT shall be carried out and completed during the period September to November of every financial year and the final report on said VAPT shall be submitted to the CDSL within one month from the date of completion of VAPT after approval from Technology Committee of respective DPs.¹⁴⁷

15.7.5 DPs are required to submit compliance of closure of findings identified during VAPT on or before April 15, 2023 for the FY 2022-2023.¹⁴⁸

¹⁴⁵ Reference: CDSL/OPS/DP/POLCY/2022/323 dated June 09, 2022

¹⁴⁶ Reference: CDSL/A,I&C/DP/POLCY/2022/331 dated June 14, 2022

¹⁴⁷ Reference: CDSL/AUDIT/DP/POLICY/2023/58 dated January 25, 2023

¹⁴⁸ Reference: CDSL/AUDIT/DP/POLICY/2023/202 dated March 31, 2023



15.8 Advisory for Cybersecurity Best Practices¹⁴⁹

Financial Computer Security Incident Response Team (CSIRT-Fin) has provided important recommendations in the form of an advisory, in its report sent to SEBI. This advisory should be read in conjunction with the applicable SEBI circulars (including but not limited to Cybersecurity and Cyber Resilience framework, Annual System Audit framework, etc.) and subsequent updates issued by SEBI from time to time.

The compliance of the advisory shall be provided by the DPs along with their cybersecurity audit report (conducted as per the applicable SEBI Cybersecurity and Cyber Resilience framework). The compliance shall be submitted as per the existing reporting mechanism and frequency of the respective cybersecurity audit.

15.9 Reporting for Artificial Intelligence (AI) and Machine Learning (ML) Applications¹⁵⁰

DPs should take note of the contents of SEBI circular no. SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 Dated January 04, 2019 regarding Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries.

DPs using AI / ML based application or system as defined in the SEBI circular, are required to make submissions in prescribed format on quarterly basis within 15 calendar days of the expiry of the quarter.

15.10 Submission of Annual System Audit Report¹⁵¹

In terms of SEBI Circular nos. SEBI/HO/MIRSD/CIR/PB/2018/147 and SEBI/HO/MIRSD/DOP/ CIR/P/2019/109 dated December 03, 2018 and October 15, 2019 respectively, the DPs are required to submit the system audit report to Depositories annually within three months of the end of the financial year.

¹⁴⁹ Reference: CDSL/OPS/DP/P OLCY/2023/133 dated March 1, 2023

¹⁵⁰ Reference: CDSL/OPS/DP/POLCY/2019/12 dated January 07, 2019 & CDSL/AUDIT/DP/POLCY/2021/302 dated July 9, 2021

¹⁵¹ Reference: CDSL/A,I&C/DP/POLCY/2022/298 May 31, 2022 & CDSL/AUDIT/DP/POLCY/2021/302 dated July 9, 2021



15.11 Framework for Adoption of Cloud Services¹⁵²

- 15.11.1 DPs are advised to refer SEBI Circular no. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023, regarding Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs).

The RE should also be aware of the new cyber security risks and challenges which cloud computing introduces. In view of the above, this cloud framework has been drafted to provide baseline standards of security and for the legal and regulatory compliances by the RE. The framework shall be seen as an addition to already existing SEBI circulars /guidelines /advisories.

The major purpose of this framework is to highlight the key risks, and mandatory control measures which REs need to put in place before adopting cloud computing. The document also sets out the regulatory and legal compliances by REs if they adopt such solutions.

The framework shall be applicable for all new or proposed cloud onboarding assignments/ projects of the REs. REs which are availing cloud services shall ensure that, wherever applicable, all such arrangements are revised and they (RE) shall be in compliance with this framework.

- 15.11.2 Additionally, the REs which are availing cloud services, shall provide milestone-based updates as follows:

- a) REs shall provide details of the cloud services, if any, currently deployed by them in the prescribed format within one month of issuance of framework
- b) The REs shall submit a roadmap (including details of major activities, timelines, etc.) for the implementation of the framework within three months of issuance of framework
- c) Quarterly progress report as per the roadmap submitted by the RE, from three to twelve months of issuance of framework
- d) Compliance with respect to the framework to be reported regularly

The above-mentioned reporting shall be done to the authority as per the existing mechanism of reporting for systems audit/ cybersecurity audit.

¹⁵² Reference: CDSL/OPS/DP/POLCY/2023/149 March 09, 2023



The cloud framework provides mandatory requirements to be fulfilled by the RE for adopting cloud computing to augment the business prospects through scalability, reduced operational cost, digital transformation and reduced IT infrastructure complexity.

- 15.11.3 This cloud framework is applicable for adoption of public cloud and community cloud. Consequently, REs are permitted to deploy public cloud and community cloud models, subject to the conditions specified herein.

A private cloud shall be considered as an on-premise deployment model and consequently, private cloud deployments shall be governed by SEBI circulars (for example cybersecurity circular, outsourcing circular, BCP-DR, etc.), guidelines, advisories, etc. issued from time to time. Therefore, private cloud deployments (by REs) are permitted, however, such deployments may not be governed by this cloud framework.

A hybrid cloud is a combination of two or more out of public cloud, community cloud and private cloud. Therefore, this cloud framework as well as the relevant SEBI circulars/ guidelines/ advisories shall be applicable for hybrid cloud deployments. In view of the above, hybrid cloud deployment is permitted, subject to the conditions specified herein.

Deployment of any other cloud model is prohibited unless explicitly permitted under this framework. However, as the field of cloud computing is a dynamic and emerging area, SEBI may allow deployment of other models after due consultations. The same may be specified by SEBI from time to time.

- 15.11.4 The cloud framework is a principle-based framework which has nine high-level principles. The framework highlights the risks associated with cloud adoption and recommends the necessary mandatory controls. The document also recommends baseline security measures required to be implemented (by RE and CSP), and RE may decide to add additional measures as per its business needs, technology risk assessment, risk appetite, compliance requirements in all the applicable circulars/ guidelines/ advisories issued by SEBI from time to time, etc.

When contemplating cloud adoption, factors including risk identification, control mechanisms, security and operational standards, vendor lock-in and compliance with the legal, technical and regulatory requirements must be taken into account.



The summary of the framework is as follows:

1. The RE may opt for any model of deployment on the basis of its business needs and technology risk assessment. However, compliance should be ensured with this cloud framework as well as other rules/ laws/ regulations/ circulars made by SEBI/ Government of India/ respective state government.
2. Although the IT services/ functionality may be outsourced (to a CSP), RE is solely accountable for all aspects related to the cloud services adopted by it including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with the laws, rules, regulations, circulars, etc. issued by SEBI/Government of India/ respective state government. Accordingly, the RE shall be responsible and accountable for any violation of the same.
3. The principles are broadly stated guidelines to set the standards by which RE must comply with while adopting cloud services. While deploying cloud services, the REs shall adopt the nine (9) principles as provided in this framework:
 - a. Principle 1: Governance, Risk and Compliance Sub-Framework
 - b. Principle 2: Selection of Cloud Service Providers
 - c. Principle 3: Data Ownership and Data Localization
 - d. Principle 4: Responsibility of the Regulated Entity
 - e. Principle 5: Due Diligence by the Regulated Entity
 - f. Principle 6: Security Controls
 - g. Principle 7: Contractual and Regulatory Obligations
 - h. Principle 8: BCP, Disaster Recovery & Cyber Resilience
 - i. Principle 9: Vendor Lock-in and Concentration Risk Management

The REs shall ensure that their cloud deployments are compliant, in letter and spirit, with the above-mentioned principles.

4. The cloud services shall be taken only from the Ministry of Electronics and Information Technology (MeitY) empaneled CSPs. The CSP's data center should hold a valid STQC (or any other equivalent agency appointed by Government of India) audit status. For selection of CSPs offering PaaS and SaaS services in India, RE shall choose only such CSPs which:
 - A) Utilize the underlying infrastructure of MeitY empaneled CSPs for providing services to the RE.
 - B) Host the application/ platform/ services provided to RE as well as store/ process data of the RE, only within the data centers as empaneled by MeitY and holding a valid STQC (or any other equivalent agency appointed by Government of India) audit status.
 - C) Have a back-to-back, clear and enforceable agreement with their partners/ vendors/ sub-contractors (including those that provide the underlying



infrastructure/ platform) for ensuring their compliance with respect to the requirements provided in this framework including those in Principles 6 (Security Controls), 7 (Contractual and Regulatory Obligations) and 8 (BCP, Disaster Recovery & Cyber resilience).

5. In a multi-tenant cloud architecture, adequate controls shall be provisioned to ensure that data (in motion, at rest and in use) shall be isolated and inaccessible to any other tenant. RE shall assess and ensure that the multi tenancy segregation controls are placed by CSP, and shall place additional security controls if required.
6. Data shall be encrypted at all lifecycle stages (at rest, in motion and in use), source or location to ensure the confidentiality, privacy and integrity.
7. RE shall retain complete ownership of all its data, encryption keys, logs etc. residing in cloud.
8. Compliance with legal and regulatory requirements, including the requirements provided in this framework, has to be ensured by the RE at all times.
9. The cloud deployments of RE shall be monitored through Security Operations Centre (SOC) [in-house, third-party SOC or a managed SOC].
10. The agreement between the RE and CSP shall cover security controls, legal and regulatory compliances, clear demarcation of roles, and liabilities, appropriate services and performance standards etc.
11. There should be an explicit and unambiguous delineation/ demarcation of responsibilities for all activities (technical, managerial, governance related, etc.) of the cloud services between the RE and CSP (and MSP/SI wherever applicable). There shall be no "joint/ shared ownership" for any function/ task/ activity between the RE and CSP. If any function/ task/ activity has to be performed jointly by the RE and CSP, there should be a clear delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) for each sub-task/ line-item within the task. The same should be a part of the agreement (as an annexure) between the RE and the CSP (and MSP/SI wherever applicable).
12. There should be an explicit and unambiguous delineation/ demarcation of responsibilities between the RE and CSP (and MSP/SI wherever applicable) for ensuring compliance with respect to circulars (for example cybersecurity and cyber resilience circular, outsourcing circular, BCP- DR etc.) issued by SEBI from time to time. There shall be no "joint/ shared ownership" for ensuring compliance with respect to any clause. If compliance for any clause has to be jointly ensured by RE and CSP (and MSP/SI wherever applicable), there should be a clear delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) for each sub- task/ line-item within the clause. This delineation shall also be added explicitly in the agreement (as an annexure) signed between the RE and the CSP (and MSP/SI wherever applicable).



13. As part of system audit of the RE, the auditor shall verify, and certify, whether there is a clear delineation/ demarcation of roles and responsibilities between the RE and CSP/MSP/SI (in-line with the “Principle 4: Responsibility of the RE” of the framework):
 - a. For each task/ function/ activity/ component.
 - b. For each clause of applicable/ relevant SEBI circular/ guidelines/ regulations
14. The auditor shall also verify, and certify, whether the above-mentioned demarcations of roles and responsibilities have been incorporated in the agreement/ contract signed between the RE and CSP (and MSP/SI wherever applicable).
15. The contractual/agreement terms between RE and CSP shall include the provisions for audit, and information access rights to the RE as well as SEBI, for the purpose of performing due diligence and carrying out supervisory reviews. RE shall also ensure that its ability to manage risks, provide supervision and comply with regulatory requirements is not hampered by the contractual terms and agreement with CSP.
16. SEBI/ CERT-In/ any other government agency shall at any time:
 - a. Conduct direct audits and inspection of resources of CSP (and its sub-contractors/ vendors) pertaining to the RE or engage third party auditor to conduct the same and check the adherence with SEBI and government guidelines/ policies/ circulars and standard industry policies.
 - b. Perform search and seizure of CSP’s resources storing/ processing data and other relevant resources (including but not limited to logs, user details, etc.) pertaining to the RE. In this process, SEBI or SEBI authorized personnel/ agency may access RE's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the CSP and/ or its sub-contractors.
 - c. Engage a forensic auditor to identify the root cause of any incident (cyber security or other incidents) related to RE.
 - d. Seek the audit reports of the audits conducted by CSP.
17. The RE shall ensure that adequate provisions are included in the agreement/ contract with CSP to enable the above functionalities. Additionally, RE shall also include provisions (in the contract/ agreement with CSP) mandating that CSP extends full cooperation to SEBI while conducting the above-mentioned activities.
18. The cloud framework should be read along with the circulars (including circulars on outsourcing, cybersecurity, BCP-DR, etc.), directions, advisories, etc. issued by SEBI from time to time.



19. The compliance with respect to the framework shall be submitted by the REs as part of their systems audit, cybersecurity audit, and VAPT reports, and no separate reporting is envisaged. The reporting shall be done as per the standardized format notified by SEBI from time to time. All other conditions for reporting (for example reporting authority, duration of reporting, etc.) shall be as per the existing mechanism of reporting for systems audit/ cybersecurity audit/VAPT.



Chapter 16 : Implementation of the Multilateral Competent Authority Agreement (MCAA) and Foreign Accounts Tax Compliance Act (FATCA)

- 16.1 DPs should take note of the contents of SEBI circular no. CIR/MIRSD/2/2015 dated August 26, 2015 regarding Implementation of the Multilateral Competent Authority Agreement and Foreign Accounts Tax Compliance Act. The Government of India has notified Rules 114F to 114H under the Income Tax Rules, 1962 and Form no, 61B for furnishing of statement of reportable accounts as specified in the Rules.

All registered intermediaries are advised to take necessary steps to ensure compliance with the requirements specified in the aforesaid Rules after carrying out necessary due diligence.¹⁵³

- 16.2 DPs should take note of SEBI circular no. CIR/MIRSD/3/2015 Dated September 10, 2015 regarding Reporting Requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)- Guidance Note. The Guidance note as mentioned in the SEBI Circular is available in the below mentioned link:
http://www.incometaxindia.gov.in/communications/notification/guidance_notes_on_implementation_31_08_2015.pdf¹⁵⁴

- 16.3 The financial institutions are advised that all efforts should be made by the financial institutions to obtain the self-certification. The account holders may be informed that, in case self-certifications are not provided till 30 April 2017, the accounts would be blocked, which would mean that the financial institution would prohibit the account holder from effecting any transaction with respect to such accounts. The transactions by the account holder in such blocked accounts may, thereafter, be permitted once the self-certification is obtained and due diligence completed.¹⁵⁵

CDSL has introduced an additional freeze reason code: No. 19 “FATCA Non Compliance (under IT Rule 114H(8))”, which the DP will be required to use at the time of blocking the accounts.¹⁵⁶

- 16.4 DPs are advised to refer to SEBI Master Circular no. SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 regarding Valid FATCA / CRS documentations to be submitted by FPI at the time of account opening.¹⁵⁷

¹⁵³ Reference: CDSL/OPS/DP/POLCY/5410 dated August 27, 2015

¹⁵⁴ Reference: CDSL/OPS/DP/POLCY/5434 dated September 11, 2015

¹⁵⁵ Reference: CDSL/OPS/DP/POLCY/196 dated April 18, 2017

¹⁵⁶ Reference: CDSL/OPS/DP/POLCY/2017/213 April 28, 2017

¹⁵⁷ Reference: CDSL/OPS/DP/POLCY/2022/733 dated December 29, 2022



Chapter 17 : Miscellaneous

17.1 Unauthenticated news circulated by DPs through various modes of communication¹⁵⁸

17.1.1 It is directed that the following monitoring mechanism to be adhered by DP in respect of unauthenticated news related to various scrips which are circulated through social media platforms/ instant messaging services/ VoIP/ blogs/chat forums/e-mail or any such medium by its employees:

- a. Proper internal code of conduct and controls are in place.
- b. Employees/temporary staff/voluntary workers etc. employed/working in the Offices of market intermediaries do not encourage or circulate rumours or unverified information obtained from client, industry, any trade or any other sources without verification.
- c. Access to Blogs/Chat forums/Messenger sites etc. is either restricted under supervision or access should not be allowed.
- d. Logs for any usage of such Blogs/Chat forums/Messenger sites (called by any nomenclature) are treated as records and the same are maintained as specified by the respective Regulations which govern the concerned intermediary.
- e. Employees are directed that any market related news received by them either in their official mail/personal mail/blog or in any other manner, should be forwarded only after the same has been seen and approved by the concerned Intermediary's Compliance Officer. If an employee fails to do so, he/she shall be deemed to have violated the various provisions contained in SEBI Act/Rules/Regulations etc. and shall be liable for actions. The Compliance Officer shall also be held liable for breach of duty in this regard.

17.2 Dealing with Conflicts of Interest¹⁵⁹

17.2.1 DPs are advised to refer to SEBI Circular no. CIR/MIRSD/5/2013 Dated August 27, 2013, in relation to general guidelines for dealing with conflicts of Interest of various Intermediaries.

DPs shall adhere to these guidelines for avoiding or dealing with or managing conflict of interest, They shall

¹⁵⁸ Reference: CDSL/OPS/DP/POLCY/2023/189 dated March 24, 2023

¹⁵⁹ Reference: CDSL/OPS/DP/POLCY/3894 dated August 29, 2013



- i. lay down, with active involvement of senior management, policies and internal procedures to identify and avoid or to deal or manage actual or potential conflict of interest, develop an internal code of conduct governing operations and formulate standards of appropriate conduct in the performance of their activities, and ensure to communicate such policies, procedures and code to all concerned;
- ii. at all times maintain high standards of integrity in the conduct of their business;
- iii. ensure fair treatment of their clients and not discriminate amongst them;
- iv. ensure that their personal interest does not, at any time conflict with their duty to their clients and client's interest always takes primacy in their advice, investment decisions and transactions;
- v. make appropriate disclosure to the clients of possible source or potential areas of conflict of interest which would impair their ability to render fair, objective and unbiased services;
- vi. endeavor to reduce opportunities for conflict through prescriptive measures such as through information barriers to block or hinder the flow of information from one department/ unit to another, etc.;
- vii. place appropriate restrictions on transactions in securities while handling a mandate of issuer or client in respect of such security so as to avoid any conflict;
- viii. not deal in securities while in possession of material non published information;
- ix. not to communicate the material non published information while dealing in securities on behalf of others;
- x. not in any way contribute to manipulate the demand for or supply of securities in the market or to influence prices of securities;
- xi. not have an incentive structure that encourages sale of products not suiting the risk profile of their clients;
- xii. not share information received from clients or pertaining to them, obtained as a result of their dealings, for their personal interest;

17.2.2 The boards of DPs shall put in place systems for implementation of this circular and provide necessary guidance enabling identification, elimination or management of conflict of interest situations. The boards shall review the compliance of this circular periodically.

The said guidelines shall be in addition to the provisions, if any, contained in respective regulations/circulars issued by the Board from time to time regarding dealing with conflict of interest, in respect of DPs.



17.3 Due Diligence in the Depository Operations¹⁶⁰

17.3.1 DPs are advised to take precautions as mentioned in the Communique while carrying out the depository operations. During the inspection of the DPs by CDSL, certain non-compliances have been observed in following areas which may expose the DPs to potential risk. In order to raise the compliance level and to mitigate the risk, DPs are advised to take note of the same:

Account opening:

1. Corrective actions are not taken by DP, for cases kept on hold/ rejected by KRA.
2. SEBI guidelines for implementation of KRA Regulations have not been followed.
3. In case of HUF account, POA is not signed by all members.
4. DP does not follow the procedure of carrying out initial KYC nor upload the information along with scanned images of KYC documents to KRA.
5. DP has not reassessed the eligibility of BOs at the end of every billing cycle and acted on SEBI circular no CIR/MRD/DP/20/2015 dated December 11, 2015 in BSDA accounts.
6. Guidelines as per SEBI circular no. CIR/MIRSD/2/2013 dated January 24, 2013 on Identification of Beneficial Ownership are not followed by DP.

Demat Related

1. Demat certificates along with rejection letters are not returned to the concerned BO within 7 days of receipt of the same from RTA.

DIS Related

1. DIS does not contain information on consideration amount/Reason/purpose in cases of transfers from one BO account to another for off-market transactions.
2. DP does not verify transactions originating from dormant accounts independently with the account holders before execution and record the details of the process on instruction slip.
3. If delivery instruction slip booklet is not issued on the basis of requisition slip, the procedure prescribed under operating instruction is not followed.
4. The delivery instructions accompanied by annexures are not accepted and processed as per the procedure prescribed by CDSL.

¹⁶⁰ Reference: CDSL/A,I&C/DP/POLCY/2019/111 dated March 01, 2019



PMLA Related

1. DP has not updated the income details of the BO in CDAS and Back office system.
2. DP does not check/monitor the transactions/ value of securities in the demat account of the BO(s) based on income and occupation details as per PMLA guidelines and follow ongoing due diligence for ensuring effectiveness of the AML procedures.
3. DP has not updated and incorporated all the points in its PMLA policy as per guidelines of PMLA and SEBI Circular SEBI/ HO/ MIRSD/ DOS3/ CIR/ P/ 2018/ 104 dated July 04, 2018.
4. DP has not categorized clients into low, medium and high risk based on perceived risk depending upon client's background, type of business activity and transactions.
5. The periodicity of review of policy is not defined in the PMLA policy.
6. PMLA policy does not have clause defining the periodicity of updating of documents taken during the client due diligence (CDD) process.

Other Areas

1. All associated persons other than those engaged in basic elementary / clerical level activities & supervised by NISM DOCE certified personnel, are not NISM-Series VI DOCE certified/ attended CPE programme as applicable to grandfathered employees.
2. Compliance Officer of the DP has not obtained NISM-Series-III A: Securities Intermediaries Compliance (Non-Fund) Certification Examination ("SICCE") as per SEBI notification dated March 11, 2013.
3. DP has not uploaded separate mobile number and e-mail address for each client as per SEBI guidelines.
4. All formats used by the DP are not in conformity with CDSL's prescribed format.
5. The DP does not use its 'easiest' login for processing of instruction(s) at least once in a month.
6. Back office software is not been used extensively for all DP activities.
7. The DPs are further advised to ensure that, in case of In-person verification (IPV), details like name of the person doing IPV, his/ her designation, organization with his/ her signatures and date are recorded on the KYC form at the time of IPV.

17.3.2 Compliance / DP officers are advised to take proper care to strengthen the internal controls and take steps to avoid such non-compliances.



List of rescinded Communiqués are as follows:

Sr. No.	Communiqué No.	Communiqué Date	Communiqué Description
Chapter 1 : Account Opening			
1	CDSL/OPS/DP/POL CY/2012/2808	16-Jan-2012	SEBI-CIRCULAR-INVESTMENT-BY-QUALIFIED-FOREIGN-INVESTORS- IN-INDIAN-EQUITY-SHARES
2	CDSL/OPS/DP/POL CY/2012/3051	8-Jun-2012	REVISION IN FRAMEWORK FOR QUALIFIED FOREIGN INVESTOR INVESTMENT IN EQUITY SHARES AND MUTUAL FUND SCHEMES
3	CDSL/OPS/DP/POL CY/2012/3203	6-Sep-2012	SEBI-CIRCULAR-KYC-REQUIREMENTS-CLARIFICATION-FOR- FOREIGN-INVESTORS
4	CDSL/OPS/DP/POL CY/2013/3921	16-Sep-2013	SEBI CIRCULAR KNOW YOUR CLIENT REQUIREMENTS FOR ELIGIBLE FOREIGN INVESTORS
5	CDSL/OPS/DP/POL CY/2014/4203	24-Jan-2014	OPERATIONAL GUIDELINES FOR DESIGNATED DEPOSITORY PARTICIPANTS
6	CDSL/OPS/DP/POL CY/2014/4370	9-Apr-2014	SEBI CIRCULAR - CHANGE IN INVESTMENT CONDITIONS-RESTRICTIONS FOR FII-QFI
7	CDSL/OPS/DP/POL CY/2014/4412	2-May-2014	SEBI CIRCULAR-INFRASTRUCTURE FACILITIES AND SUBMISSION OF PERIODIC REPORTS BY DDPS
8	CDSL/OPS/DP/POL CY/2014/4506	17-Jun-2014	SEBI CIRCULAR- KNOW YOUR CLIENT -KYC- REQUIREMENTS FOR FOREIGN PORTFOLIO INVESTORS - FPIS
9	CDSL/OPS/DP/POL CY/2015/4979	5-Feb-2015	CHANGE IN INVESTMENT CONDITIONS RESTRICTIONS FOR FPI INVESTMENTS IN CORPORATE DEBT SECURITIES
10	CDSL/OPS/DP/POL CY/2015/4983	6-Feb-2015	CHANGE IN INVESTMENT CONDITIONS FOR FPI INVESTMENTS IN GOVERNMENT DEBT SECURITIES



Sr. No.	Communiqué No.	Communiqué Date	Communiqué Description
11	CDSL/OPS/DP/POL CY/2015/5487	8-Oct-2015	SEBI CIRCULAR INVESTMENTS BY FPIS IN GOVERNMENT SECURITIES
12	CDSL/OPS/DP/POL CY/2016/5821	17-Mar-2016	INVESTMENTS BY FPIS IN REITS INVITS AIFS AND CORPORATE BONDS UNDER DEFAULT
13	CDSL/OPS/DP/POL CY/2016/6061	5-Aug-2016	FOREIGN INVESTMENT IN RUPEE DENOMINATED BONDS
14	CDSL/OPS/DP/POL CY/2016/6170	4-Oct-2016	SEBI CIRCULAR INVESTMENTS BY FPIS IN GOVERNMENT SECURITIES
15	CDSL/OPS/DP/POL CY/2016/6253	21-Nov-2016	SEBI CIRCULAR FPIS REQUIREMENT OF PAN
16	CDSL/OPS/DP/POL CY/2017/15	5-Jan-2017	SEBI CIRCULAR GUIDELINES PARTICIPATION FUNCTIONING FPI IN IFSC
17	CDSL/OPS/DP/POL CY/2017/59	1-Feb-2017	SEBI CIRCULAR CREDIT OF PROCEEDS DUE TO WRITE OFF OF SECURITIES HELD BY FPI
18	CDSL/OPS/DP/POL CY/2017/116	3-Mar-2017	SEBI CIRCULAR INVESTMENTS BY FPIS IN CORPORATE DEBT SECURITIES
19	CDSL/OPS/DP/POL CY/2017/332	5-Jul-2017	SEBI CIRCULAR -INVESTMENTS BY FPIS IN GOVERNMENT SECURITIES
20	CDSL/OPS/DP/POL CY/2017/333	5-Jul-2017	SEBI CIRCULAR ACCEPTANCE OF E-PAN CARD FOR KYC PURPOSE FOR FPIS
21	CDSL/OPS/DP/POL CY/2017/347	13-Jul-2017	SEBI CIRCULAR FPI IFSC AMENDMENTS
22	CDSL/OPS/DP/POL CY/2017/364	24-Jul-2017	INVESTMENTS BY FPIS IN CORPORATE DEBT
23	CDSL/OPS/DP/POL CY/2017/487	5-Oct-2017	SEBI CIRCULAR INVESTMENTS BY FPIS IN GOVERNMENT SECURITIES
24	CDSL/OPS/DP/POL CY/2017/551	17-Nov-2017	SEBI CIRCULAR INVESTMENTS BY FPIS IN HYBRID SECURITIES
25	CDSL/OPS/DP/POL CY/2017/608	21-Dec-2017	SEBI CIRCULAR INVESTMENTS BY FPIS IN GOVERNMENT SECURITIES



Sr. No.	Communiqué No.	Communiqué Date	Communiqué Description
26	CDSL/OPS/DP/POL CY/2018/81	17-Feb-2018	SEBI CIRCULAR EASING OF ACCESS NORMS FOR INVESTMENT BY FPIS
27	CDSL/OPS/DP/POL CY/2018/122	12-Mar-2018	SEBI CIRCULAR SEPARATE LIMIT OF INTEREST RATE FUTURES IRFS FOR FPIS
28	CDSL/OPS/DP/POL CY/2018/125	14-Mar-2018	CLARIFICATIONS IN RESPECT OF INVESTMENT BY CERTAIN CATEGORY II FPIS
29	CDSL/OPS/DP/POL CY/2018/193	11-Apr-2018	SEBI CIRCULAR - KNOW YOUR CLIENT REQUIREMENTS FOR FOREIGN PORTFOLIO INVESTORS
30	CDSL/OPS/DP/POL CY/2018/192	11-Apr-2018	SEBI CIRCULAR - CLARIFICATION ON CLUBBING OF INVESTMENT LIMITS OF FOREIGN GOVERNMENT
31	CDSL/OPS/DP/POL CY/2018/202	16-Apr-2018	INVESTMENTS BY FPIS IN GOVERNMENT AND CORPORATE DEBT SECURITIES
32	CDSL/OPS/DP/POL CY/2018/314	18-Jun-2018	SEBI CIRCULAR REVIEW OF INVESTMENT BY FOREIGN PORTFOLIO INVESTORS FPI IN DEBT
33	CDSL/OPS/DP/POL CY/2018/368	13-Jul-2018	SEBI CIRCULAR INVESTMENT BY FPI THROUGH PRIMARY MARKET ISSUANCES
34	CDSL/OPS/DP/POL CY/2018/448	24-Aug-2018	SEBI CIRCULAR AMENDMENT TO KNOW YOUR CLIENT REQUIREMENTS FOR FPIS
35	CDSL/OPS/DP/POL CY/2018/506	24-Sep-2018	SEBI CIRCULAR ELIGIBILITY CONDITIONS FOR FOREIGN PORTFOLIO INVESTORS
36	CDSL/OPS/DP/POL CY/2018/507	24-Sep-2018	SEBI CIRCULAR KNOW YOUR CLIENT REQUIREMENTS FOR FOREIGN PORTFOLIO INVESTORS
37	CDSL/OPS/DP/POL CY/2018/548	16-Oct-2018	SEBI CIRCULAR MONTHLY REPORT OF FPI REGISTRATION ON SEBIS WEBSITE



Sr. No.	Communiqué No.	Communiqué Date	Communiqué Description
38	CDSL/OPS/DP/POL CY/2018/666	14-Dec-2018	SEBI CIRCULAR CLARIFICATION ON CLUBBING OF INVESTMENT LIMITS OF FPI
39	CDSL/OPS/DP/POL CY/2019/140	15-Mar-2019	SEBI CIRCULAR REVIEW OF INVESTMENT BY FPI IN DEBT
40	CDSL/OPS/DP/POL CY/2019/234	10-May-2019	SEBI CIRCULAR PERMITTING FPI TO INVEST IN MUNICIPAL BONDS
41	CDSL/OPS/DP/POL CY/2019/561	6-Nov-2019	SEBI CIRCULAR - OPERATIONAL GUIDELINES FOR FPIS
42	CDSL/OPS/DP/POL CY/2020/85	12-Feb-2020	COMMON APPLICATION FORM FOR FOREIGN PORTFOLIO INVESTORS
43	CDSL/OPS/DP/POL CY/2020/414	24-Sep-2020	WRITE OFF OF SHARES HELD BY FPIS
44	CDSL/OPS/DP/POL CY/2021/149	1-Apr-2021	GUIDELINES PERTAINING TO SURRENDER OF FPI REGISTRATION
45	CDSL/OPS/DP/POL CY/2021/248	2-Jun-2021	OFF MARKET TRANSFER OF SECURITIES BY FPI
46	CDSL/OPS/DP/POL CY/2021/379	31-Aug-2021	MODIFICATION IN OPERATIONAL GUIDELINES FOR FPIS AND DDPS
47	CDSL/OPS/DP/POL CY/2021/507	10-Nov-2021	SEBI - WRITE OFF OF DEBT SECURITIES HELD BY FPIS SURRENDERING THEIR REGISTRATION
48	CDSL/OPS/DP/POL CY/2022/243	4-May-2022	MODIFICATION IN THE OPERATIONAL GUIDELINES FOR FPI DDP ELIGIBLE FOREIGN INVESTORS
49	CDSL/OPS/DP/POL CY/2022/348	22-Jun-2022	MODIFICATION IN OPERATIONAL GUIDELINES FOR FPIS, DDPS AND ELIGIBLE FOREIGN INVESTORS
50	CDSL/OPS/DP/POL CY/2022/556	28-Sep-2022	MODIFICATION IN THE OPERATIONAL GUIDELINES FOR FPIS, DDPS AND EFIS



Sr. No.	Communiqué No.	Communiqué Date	Communiqué Description
Chapter 2 : Account Modification			
51	CDSL/OPS/DP/1454	5-Feb-2009	PAN MODIFICATION EXCLUSIVELY AT CDSL-END.
52	CDSL/OPS/DP/1459	10-Feb-2009	PAN MODIFICATION AT CDSL END
53	CDSL/OPS/DP/1467	12-Feb-2009	PAN MODIFICATION AT CDSL-END
54	CDSL/OPS/DP/1519	26-Mar-2009	PAN MODIFICATION AT CDSL'S END
55	CDSL/OPS/DP/ACC TS/2910	20-Mar-2012	PAN MODIFICATION AT CDSL END
56	CDSL/OPS/DP/ACC TS/6040	26-Jul-2016	PAN MODIFICATION AT CDSL.S END
Chapter 7 : Freeze / Unfreeze			
57	CDSL/OPS/DP/817	3-Jan-2007	UNFREEZE-OPTION-FOR-ENTERING-PAN AND RE-ACTIVATION.
Chapter 10 : Internal Controls / Reporting to CDSL			
58	CDSL/OPS/DP/POL CY/2022/524	14-Sep-2022	MASTER CIRCULAR ON SURVEILLANCE OF SECURITIES MARKET
59	CDSL/OPS/DP/POL CY/2596	8-Aug-2011	REVISED PROCEDURE FOR SEEKING PRIOR APPROVAL FOR CHANGE IN CONTROL THROUGH SINGLE WINDOW
Chapter 14 : Prevention of Money Laundering Act, 2002 (PMLA)			
60	CDSL/OPS/DP/649	23-Jan-2006	GUIDELINES ON ANTI MONEY LAUNDERING MEASURES
61	CDSL/OPS/DP/1408	31-Dec-2008	GUIDELINES ON ANTI MONEY LAUNDERING MEASURES
62	CDSL/OPS/DP/1706	4-Sep-2009	GUIDELINES ON ANTI-MONEY LAUNDERING MEASURES
63	CDSL/OPS/DP/1751	24-Oct-2009	PROCEDURE FOR IMPLEMENTATION OF SECTION 51A OF THE UNLAWFUL ACTIVITIES -PREVENTION ACT- 1967
64	CDSL/OPS/DP/1751	18-Feb-2010	GUIDELINES ON ANTI-MONEY LAUNDERING MEASURES
65	CDSL/OPS/DP/2236	6-Jan-2011	SEBI CIRCULAR ANTI MONEY LAUNDERING COMBATING FINANCING



Sr. No.	Communiqué No.	Communiqué Date	Communiqué Description
			OF TERRORISM STANDARDS MASTER CIRCULAR
66	CDSL/OPS/DP/POL CY/4309	13-Mar-2014	SEBI CIRCULAR- ON ANTI-MONEY LAUNDERING
67	CDSL/OPS/DP/POL CY/2018/352	7-Jul-2018	SEBI CIRCULAR GUIDELINES ON AML STANDARDS AND COMBATING THE FINANCING OF TERRORISM (CFT
68	CDSL/OPS/DP/POL CY/2019/263	29-May-2019	SEBI CIRCULAR CFT UNDER UNLAWFUL ACTIVITIES PREVENTION ACT 1967
69	CDSL/OPS/DP/P OLCY/2019/542	25-Oct-2019	ANTI MONEY LAUNDERING COMBATING FINANCING OF TERRORISM STANDARDS
70	CDSL/AUDIT/DP/P OLCY/2021/160	7-Apr-2021	COMBATING FINANCING OF TERRORISM
Chapter 16 : Implementation of the Multilateral Competent Authority Agreement (MCAA) and Foreign Accounts Tax Compliance Act (FATCA)			
71	CDSL/OPS/DP/POL CY/2018/169	2-Apr-2018	DUE DILIGENCE AND REPORTING UNDER FATCA AND COMMON REPORTING STANDARDS
Chapter 17 : Miscellaneous			
72	CDSL/OPS/DP/POL CY/2370 March 24, 2011	24-Mar-2011	UNAUTHENTICATED NEWS CIRCULATED BY SEBI REGISTERED MARKET INTERMEDIARIES THROUGH VARIOUS MODES OF COMMUNICATION