## X. REPORTING REQUIREMENTS

| S No. | Para No. of the Master circular | Reporting requirement |
|---|---|---|
| **Reporting to Stock Exchanges** | | |
| 1. | 13.2 | The member shall carry out complete internal audit on a half yearly basis and shall forward the report along with para-wise comments to the respective Stock Exchange/ Clearing Corporation within two months from the end of the half year period. |
| 2. | 15.4.1 | The stock brokers shall inform the Stock Exchanges of existing and new bank account(s) in the format specified at Table 2. |
| 3. | 15.4.2 | The stock brokers shall inform the Stock Exchanges of existing and new demat account(s) in the format specified at Table 3. |
| 4. | 15.5.2 | The uploading of the data (specified at 15.5.2) by the stock broker to the Stock Exchanges shall be on weekly basis i.e. stock brokers shall submit the data as on last trading day of every week on or before the next three trading days. |
| 5. | 15.6.5.1 | Stock Brokers shall ensure that the internal audit reports are submitted to the Exchanges within two months of the end of respective half years for which the audit is being conducted. |
| 6. | 15.7.2 | Stock Brokers shall submit financial statements to Stock Exchanges in the same format as prescribed under the Companies Act, 2013 irrespective of whether they fall under the purview of the Companies Act, 2013 or not. The due date for submission of the aforesaid financial statements to Stock Exchanges shall be the same as prescribed under the Companies Act, 2013 for submission to Registrar of Companies. |
| 7. | 15.9.1 | The Stock Brokers shall upload the data (specified at para 15.9.1) on a monthly basis for every client onto each Stock Exchange system where the broker is a member |
| 8. | 19.2.2 | The brokers shall be required to furnish the particulars (mentioned at para 19.1 and 19.2.1) of their clients to the Stock Exchanges/Clearing Corporations and the same would be updated on a monthly basis. Such information for a specific month should reach the exchange within seven working days of the following month. |

| | | |
|---|---|---|
| 9. | 22.9 | As on 31st March of every year, a statement of balance of Funds and Securities in hard form and signed by the broker shall be sent to all the clients. |
| 10. | 33.2.2 | Stock Brokers shall upload the details of clients, such as, name, mobile number, address for correspondence and E-mail address to Stock Exchanges |
| 11. | 38.4.3 | The stock brokers shall submit to the Stock Exchange a half-yearly certificate, as on 31st March and 30th September of each year, from an auditor confirming the net worth. Such a certificate shall be submitted not later than 30th April and 31st October of every year. |
| 12. | 38.7.1 | The stock broker shall disclose to the Stock Exchanges details on gross exposure towards margin trading facility including name of the client, Category of holding (Promoter/promoter group or Non-promoter), clients' PAN, name of the scrips (Collateral stocks and Funded stocks) and if the stock broker has borrowed funds for the purpose of providing margin trading facility, name of the lender and amount borrowed, on or before 12 noon on the following trading day. The format for this disclosure by the stock broker to the stock exchange is enclosed at Annexure-15. |
| 13. | 38.9.3 | The books of accounts, maintained by the broker, with respect to the margin trading facility offered by it, shall be audited on a half yearly basis. The stock broker shall submit an auditor's certificate to the exchange within one month from the date of the half year ending 31st March and 30th September of a year certifying, inter alia, the extent of compliance with the conditions of margin trading facility. |
| 14. | 42.2 | On a daily basis,<br>• TM shall report disaggregated information on collaterals up to the level of its clients to the CM.<br>• CM shall report disaggregated information on collaterals up to the level of clients of TM and proprietary collaterals of the TMs to the Stock Exchanges (SEs) and CCs in respect of each segment. |
| 15. | 55.5 & 55.6 | The stock brokers / trading members that provide the facility of algorithmic trading shall subject their algorithmic trading system to a system audit every six months in order to ensure that the requirements prescribed by SEBI / stock exchanges |

| | | |
|---|---|---|
| | | with regard to algorithmic trading are effectively implemented.<br>Deficiencies or issues identified during the process of system audit of trading algorithm / software shall be reported by the stock broker / trading member to the stock exchange immediately on completion of the system audit. |
| 16. | 59.4 | All registered Stock Brokers using AI / ML based application or system as defined in Annexure 26, are required to fill in the form (Annexure 25) and make submissions on quarterly basis within fifteen calendar days of the expiry of the quarter. |
| 17. | 72.3 | Stock Brokers shall disclose on their respective websites, the data on complaints received against them or against issues dealt by them and redressal thereof, latest by seventh of succeeding month, as per the format enclosed at Annexure-37. |
| 18. | 86.3 | The URL to the website of a stock broker shall be reported to the stock exchanges within a week of the provisions at para 86.1 of this master circular, coming into effect. Any modification in the URL shall be reported to stock exchanges within 3 days of such changes. |
| **Reporting to clients** | | |
| 19. | 15.10.1.6 & 47.8 | Once the TM settles the running account of funds of a client, an intimation shall be sent to the client by SMS on mobile number and also by email. The intimation should also include details about the transfer of funds (in case of electronic transfer – transaction number and date; in case of physical payment instruments – instrument number and date). TM shall send the retention statement along with the statement of running accounts to the clients as per the existing provisions within five working days. |
| 20. | 48.3.7.a | In addition to the e-mail communication of the ECNs in the manner stated above, in order to further strengthen the electronic communication channel, the member shall simultaneously publish the ECN on his designated web-site in a secured way and enable relevant access to the clients. |
| 21. | 49.2.2.e.i | Contract notes must be issued to clients as per existing regulations, within twenty-four hours of the trade execution. |
| 22. | 71.1 | For information of all investors who deal/ invest/ transact in the market, the offices of all stock brokers (and its authorized person(s)) shall prominently display basic information, as |

| | | |
|---|---|---|
| | | provided in Annexure-35, about the grievance redressal mechanism available to investors. |
| 23. | 72.2 | Stock Brokers shall bring the Investor Charter to the notice of their clients (existing as well as new clients) through disclosing the Investor Charter on their respective websites, making them available at prominent places in the office, provide a copy of Investor Charter as a part of account opening kit to the clients, through e-mails/ letters etc. |
| **Technology related reporting requirements** | | |
| 24. | 16-Table – 8 (1.5) | The system audit report submitted by the auditor should be forwarded to the Stock Exchange by the Stock Broker along with management comments, within one month of submission of report by the auditor. |
| 25. | 18.5.5.14 | QSBs shall arrange to have their systems audited on half-yearly basis by a CERT-IN empanelled auditor to check compliance with the above mentioned requirements related to cyber security and other circulars of SEBI on cybersecurity and technical glitches, to the extent they are relevant to them and shall submit the report to stock exchanges along with the comments of the cybersecurity committee within one month of completion of the half year. |
| 26. | 53.4.7 | A systems audit of the DMA systems and software shall be periodically carried out by the broker as may be specified by the exchange and certificate in this regard shall be submitted to the exchange. |
| 27. | 54.2.13 | System audit of the Smart Order Routing systems and software shall be periodically carried out by the brokers as may be specified by the exchange and certificate in this regard shall be submitted to the exchange. |
| 28. | 58.2 | The Stock Brokers are mandated to conduct comprehensive cyber audit at least once in a financial year. All Stock Brokers shall submit with Stock Exchange a declaration from the MD/ CEO/ Partners/ Proprietors certifying compliance by the Stock Brokers with all SEBI Circulars and advisories related to Cyber security from time to time, along with the Cyber audit report. |
| 29. | 58.44 | Stock Brokers shall conduct VAPT at least once in a financial year. All Stock Brokers are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock |

| | | |
|---|---|---|
| | | Exchanges after approval from Technology Committee of respective Stock Brokers, within 1 month of completion of VAPT activity. |
| 30. | 58.54 | All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers shall be reported to Stock Exchanges & SEBI within six hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in. |
| 31. | 58.55 | 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 Stock Brokers, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.<br><br>The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Exchanges and SEBI, shall be submitted to Stock Exchanges within 15 days from the quarter ended June, September, December and March of every year (Format for Submitting the reports is attached in below Annexure 24). |
| 32. | 58.62 | The Type I Stock Brokers shall arrange to have their systems audited on an annual basis by a CERT-IN empanelled auditor, an independent DISA (ICAI) Qualification, CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (commonly known as (ISC)2), to check compliance with the above areas and shall submit the report to Stock Exchanges along with the comments of the Board / Partners / Proprietor of Stock Broker within three months of the end of the financial year. |

| | | |
|---|---|---|
| 33. | 60.4 | The compliance of the advisory shall be reported in the half yearly report by stock brokers to stock exchanges with an undertaking, "Compliance of the SEBI circular for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions has been made." |
| 34. | 61.3.1 | Stock brokers shall inform about the technical glitch to the stock exchanges immediately but not later than one hour from the time of occurrence of the glitch. |
| 35. | 61.3.2 | Stock brokers shall submit a Preliminary Incident Report to the Exchange within T+1 day of the incident (T being the date of the incident). The report shall include the date and time of the incident, the details of the incident, effect of the incident and the immediate action taken to rectify the problem. |
| 36. | 61.3.3 | Stock brokers shall submit a Root Cause Analysis (RCA) Report (as per Annexure 29) of the technical glitch to stock exchange, within fourteen days from the date of the incident. |
| 37. | 61.3.5 | Stock brokers shall submit information stated in para 61.3.1, 61.3.2 and 61.3.3 above, by e-mail at infotechglitch@nse.co.in, a common email address for reporting across all stock exchanges. |
| 38. | 62.5 | The compliance of the advisory shall be provided by the REs 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. |
| **Reporting requirements for QSBs** | | |
| 39. | 18.5.1.3 | QSBs shall submit an annual report to the stock exchanges regarding the observations of the committees of BOD or analogous body, corrective action taken by the QSB and measures taken to prevent recurrence of such incidents. |
| 40. | 18.5.2.3 | The risk management framework shall have measures for carrying out surveillance of client behaviour through analyzing the pattern of trading done by clients, detection of any unusual activity being done by such clients, reporting the same to stock exchanges. |
| 41. | 18.5.2.8 | The risk management policy shall be reviewed on half yearly basis by the QSB and a report in this regard shall be submitted by the risk management committee of the QSB to the stock exchange. |

| | | |
|---|---|---|
| 42. | 18.5.5.14 | QSBs shall arrange to have their systems audited on half-yearly basis by a CERT-IN empanelled auditor to check compliance with the above mentioned requirements related to cyber security and other circulars of SEBI on cybersecurity and technical glitches, to the extent they are relevant to them and shall submit the report to stock exchanges along with the comments of the cybersecurity committee within one month of completion of the half year. |
| **Other reporting requirements** | | |
| 43. | 80.6.1 | Reporting to Financial Intelligence Unit (FIU) - The stock brokers 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. |

## Annexures

### Annexure-1

1. Name of the Stock Exchange
2. Name of the Applicant Member Broker
3. Exchange Clearing Code No. (If allotted by the Stock Exchange)
4. Trade Name of Member
5. Address of Member

   Tel. No. (O):
   Tel No. (R):
   Fax No.

6. Form of Organisation: Please tick the relevant entity
   6.1 Partnership
   6.2 Corporate Body
      a. Financial Institution
      b. Others
      c. Foreign Joint Ventures

   (If an Indian Company is holding more than 25% of total equity in the joint venture, please give details of top five shareholders of Indian Company).

| **Name of Indian Company** | |
|---|---|
| Top five Shareholders | % Holding |
| **1** | |
| **2** | |
| **3** | |
| **4** | |
| **5** | |
| FIPB Approval, if applicable | |

**Sole Proprietorship:**

| **Name of proprietor** | **Educational Qualification** | **Age (on the date of filing of application)** | **Experience (specify the nature and years)** |
|---|---|---|---|
| | | | |

**Partnership:**

| **Name of partners** | **Age (on the date of application)** | **Educational Qualification** | **Experience (specify the nature and years)** | **In case partner(s) is/are registered with SEBI,** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | | | | **give SEBI Regd. No.** |
| | | | | |

**Corporate Body (Financial Institution /Others)**

MOA object clause contains stock broking as one of the object in

Main Object
Other Object
Incidental Object

(If, stock broking clause appears in other object please attach a copy of special resolution to amend the MOA to incorporate Stock Broking in main object clause)

Mention relevant clause no. (Please enclose copy of the relevant clause of the MOA duly certified by the Stock Exchange. **If certified copy is not enclosed application would be returned**).

Information regarding directors

| **Name of directors with designation (whether whole time/designated/ additional** | **Percentage of Share holding** | **Educational Qualification** | **Experience (specify nature and years)** | **Whether directors in other corporate bodies engaged in capital markets (please give names and SEBI Regd. No.)** |
|---|---|---|---|---|
| | | | | |

Details of top five shareholders

| **Name of shareholders** | **Percentage of Share holding** | **Educational Qualification** | **Experience (specify nature and years)** | **Whether shareholders in other corporate bodies engaged in capital markets (please give names and SEBI Regd. No.)** |
|---|---|---|---|---|
| | | | | |

7. Date of Admission to Membership of the Stock Exchange.

8. Mode of Acquiring Membership (Please attach old SEBI Registration certificate in all cases other than the cases of new membership)
   8.1 New Membership
   8.2 Conversion
   8.3 Succession
   8.4 Auction Purchase
   (In case member has become defaulter)
   8.5 Market Purchase
   8.6 Transfer to another Company under same management
   (please specify reasons)
   8.7 Others, please specify

9. Please give the following information in all the cases other than the case of new membership
   9.1 Name of the previous holder of the card
   9.2 SEBI Registration No.
   9.3 Date of Registration with SEBI

10. Whether the applicant is member of more than one Stock Exchange? YES/ NO

11. If yes, please give name(s) of the Stock Exchange(s) with Code No. and SEBI registration no.

12. Whether any of the Associate Companies/Partnership/ Proprietorship Firm is /are having direct/indirect interest (* as defined below) in capital market? YES / NO

* The member is deemed to have direct/indirect interest in the following conditions:

   12.1 Where he is individual, he or any of his relative being a broker/any intermediary, he or any of his relative being a partner in a broking firm/any intermediary, he or any of his relative being a director in a broking company/any intermediary or he or any of his relatives clubbed together holding substantial equity in any broking company/any intermediary engaged in capital market.

   12.2 Where it is partnership firm/company, the relative(s) of partner(s)/director(s) in the firm(s)/corporate body being a broker/any intermediary or being partner(s)/director(s) in any broking/intermediary or the same set of shareholders holding substantial equity in other broking / any intermediary engaged in capital market.

   12.3 Relative shall mean husband, wife, brother, unmarried sister or any linear ascendant or descendant of an individual.

   12.4 If yes, please give details (you may attach separate sheet, if required)

| Name | Form of Organisation | Type of Intermediary# | Whether registered with SEBI (give Regd. No.) | Nature of interest |
|---|---|---|---|---|
| | | | | |

# Merchant Banker, Portfolio Manager, Registrar to Issue & Share Transfer Agent, Banker to an Issue, Mutual Fund, Venture Capital , Underwriter, Debenture Trustee, FII.

13. Disciplinary Action initiated/taken against the Associate entities, as indicated in 12.4 above. (Please state details of nature of violation, action initiated/taken and by which authority)

    13.1 Disciplinary action taken by SEBI (if yes, please attach details mentioning nature of violation and action taken) YES / NO

    13.2 Disciplinary action taken by any other authority (please attach details of nature of violation and action initiated) YES / NO

    13.3 Disciplinary action initiated by SEBI (if yes, please attach details of nature of violation and action taken) YES / NO

    13.4 Disciplinary action initiated by any other authority (please attach details of nature of violation and action initiated ) YES / NO

14. Net-worth as per the requirement of the exchange (Rs in Lakhs)

15. Applicant's net-worth as prescribed in SEBI (Stock Brokers) Regulations, 1992 (Rs in Lakhs) (Certificate from a qualified CA certifying the above should be enclosed)

I/we declare that the information given in this form is true to the best of my knowledge and belief.

**Date: Signature**

**Name and Address of the applicant**

**List of Enclosures:**

a. Registration fees –Rs 50,000/- payable by the applicant by way of direct credit in the bank account through online payment using SEBI payment gateway.[103]

[103] Amended by the SEBI (Payment of Fees and Mode of Payment) (Amendment) (Regulations) 2021 w.e.f. 05-05-2021

b. Copy of relevant clause of MOA duly certified by the Stock Exchange.
c. Certificate from the qualified Chartered Accountant certifying the networth and paid up capital.
d. Undertaking by applicant that he/ it had not introduced through any member brokerof the Exchange any fake/forged/stolen shares in the Exchange/market. If yes, details thereof including action taken, if any, by the applicant.

**Certification by Stock Exchange**

The above details have been scrutinized as per record made available to the Stock Exchange.

**SIGNATURE:**

**NAME:**

**DESIGNATION:**

**SEAL OF STOCK EXCHANGE**

**Certification from the Stock Exchange:**

This is to certify that
i) The member is eligible to be admitted as the member of the Exchange as per the provisions of SC(R)A, SC(R)R, bye-laws of the exchange and circulars issued by Government of India and SEBI, in particular the GOI guidelines dated November 09, 1989 and SEBI circular dated May 14, 1993.
ii) ---------- is admitted as a member of this exchange as approved by the Council of Management in its meeting held on _.
iii) No complaints/ arbitration cases/ disciplinary action are pending against the transferor M/s _ and all the complaints received by the Exchange or referred by SEBI have been settled to the satisfaction of the Stock Exchange.
iv) We have verified the educational qualification, age, experience of the member with respect to the original record and found it to be correct as per the information given in the application.
v) No litigation with regard to transfer of card is pending in court of law.

The application is recommended for registration with the Securities and Exchange Board of India under Securities and Exchange Board of India (Stock Brokers) Regulations, 1992.

**Signature:**

**Name:**

**Designation:**

**List of Enclosures along with application:**

1. Turnover fee details of the transferor in the prescribed format (enclosed).
2. Disciplinary record of the transferor
3. Board Resolution approving the membership (will be submitted by the Exchange)

## Annexure-2[104]

| The common irregularities observed in the Stock Brokers/trading members books are brought to the notice of all. They are as follows: | |
|---|---|
| **S. No.** | **Description** |
| I | **Relating to KYC**<br><br>1. 'In person verification' not done while opening the account. Photo copy of KYC &Rights and Obligations document are not provided to clients; if provided proof of delivery/dispatch is not maintained.<br><br>2. Adding clauses in Rights and Obligations document which are contrary to the clauses as prescribed by SEBI. Voluntary clauses are not highlighted as 'voluntary' and signatures of clients taken on all the documents. |
| II | **Relating to Contract notes**<br><br>3. Contract notes are not bearing serial numbers, SEBI registration numbers, Order no. & time. Contract notes are not issued in the prescribed format/not issued within twenty-hours of trade execution/not signed properly by the broker or his authorized representatives.<br><br>4. Duplicates/counterfoils/acknowledged copies of the contract notes issued not being maintained or maintained with inadequate details.<br><br>5. Not issuing contracts in the prescribed format while acting as principal.<br><br>6. Appropriate stamp duty not paid and charging Securities Transaction Tax (STT) on non-equity funds transactions by the brokers.<br><br>7. Brokerage is not shown separately on contract notes. The correct rate at which the transaction was executed is not passed on to the client.<br><br>8. Charges other than brokerage and statutory charges levied on the clients which are not specifically agreed upon by the clients or charging more than the limits prescribed.<br><br>9. In case the Electronic Contract Notes (ECN) are issued, the same are not made available on brokers' websites/ sending ECN on single email-id for a group of clients/not maintaining ECN logs for ECN sent to the clients. |

[104] Para VI(37) of Annexure of Circular SEBI/MIRSD/MASTER CIR-04/2010 dated March 17, 2010, deleted in view of Notification LAD-NRO/GN/2011-12/03/12650 dated April 19, 2011.

| | |
|---|---|
| III | **Relating to Investor services**<br><br>10. Deficiency in service to the clients.<br><br>11. Non maintenance of investor grievance register and lack of proper system for receipt and reconciliation of investor grievances/not taking adequate steps for redressal of grievances of investors within one month from the date of receipt of the complaint.<br><br>12. Non maintenance of client database or details captured wrongly in the database.<br><br>13. There are delays between pay-out by the exchange to their members and the transmission of shares/money received in such pay-out to their clients by brokers without any record of reasons for such delay.<br><br>14. Non dissemination of email ID created for receiving investor grievances to the investors.<br><br>15. Freezing of accounts of clients without giving adequate reason.<br><br>16. Providing multiple client codes to one client/using same PAN no. for more than one client.<br><br>17. Frequent trade modification/client code modification done in client account<br><br>18. Daily margin statement and quarterly statements not sent to clients<br><br>19. Relationship managers acting as portfolio managers by entering into verbal agreement with clients for trading on their behalf. |
| IV | **Relating to funds and securities**<br><br>20. Unauthorized trading activities carried out in client's account.<br><br>21. Not having separate account for clients' funds/securities or having separate accounts for clients but not segregating clients' funds/securities from its own funds/securities.<br><br>22. The brokers are found involved in funding activities - with the exception of those in connection with or incidental to or consequential upon the securities business.<br><br>23. Non collection of margin from clients/wrong reporting of collection of margins to exchanges/clearing members. |

| | |
|---|---|
| | 24. Accepting cash from the clients. Accepting/giving third party payments/receipts. |
| V | **Relating to terminals**<br><br>25. Not putting the unique client code (UCC) of clients while placing orders in the trading system.<br><br>26. The broker granting the trading terminals at places other than that specified by SEBI e.g. registered office, branch office.<br><br>27. Terminals operated by personnel without having proper qualification/ persons operating the terminal are not employees/remisiers. |
| VI | **Others**<br><br>28. Non-maintenance or improper maintenance of Books of Accounts which are required to be maintained as per Rule 15 of SCRA Rules 1957 and Regulation 17 of Stock Brokers Regulations 1992.<br><br>29. Non-compliance with provisions relating to spot/negotiated deals.<br><br>30. Instances of the broker/dealers/others connected with the broker, involved in front running, circular trading, creating false markets, misuse of the exchange mechanism for securing financing transactions, entering fictitious transactions and illegal transactions.<br><br>31. Non submission of audit report/internal audit reports within the prescribed time limit.<br><br>32. Involved in business other than the securities business in violation of applicable laws.<br><br>33. Non-payment/ inadequate payment of SEBI registration fees by the stock brokers.<br><br>34. Not complying with the provisions of advertisements/internet based trading<br><br>35. Non appointment of compliance officer.<br><br>36. Non- compliance with trading restrictions imposed by Stock Exchanges<br><br>37. Trading in unlisted securities and in securities prior to their admission to dealings by Exchanges |

| | |
|---|---|
| | 38. Not reporting off-the-floor transactions (e.g.) (a) The transactions with stock brokers of other exchanges (b) Principal to principal transactions with clients (c) Transactions done after the trading hours.<br><br>39. Non-formation of policies related to internal controls, employee/insider trading, Prevention of Money Laundering (PML) etc. If policies are formulated, they are not implemented.<br><br>40. Delivery vs payment (DvP) trades are done in other than those circumstances as prescribed. |

## Annexure-3

**1. Terms of Reference (ToR) for Type I Broker**

The system auditor shall at the minimum cover the following areas:

1.1. **System controls and capabilities**

1.1.1. **Order Tracking** – The system auditor should verify system process and controls at exchange provided terminals with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.

1.1.2. **Order Status/ Capture** – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.

1.1.3. **Rejection of orders** – Whether system has capability to reject orders which do not go through order level validation at the end of the stock broker and at the servers of respective Stock Exchanges.

1.1.4. **Communication of Trade Confirmation / Order Status** – Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.

1.1.5. **Client ID Verification** – Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.

1.2. **Risk Management System (RMS)**

1.2.1. **Online risk management capability** – The system auditor should check whether the system of online risk management (including upfront real-time risk management) is in place for all orders placed through exchange provided terminals.

1.2.2. **Trading Limits** –Whether a system of pre-defined limits / checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc) are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.

1.2.3. **Order Alerts and Reports** –Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to Margin Requirements, payments and delivery obligations.

1.2.4. **Order Review** –Whether the system has capability to facilitate review of such orders were not validated by the system.

1.2.5. **Back testing for effectiveness of RMS** – Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.

1.2.6. **Log Management** – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

1.3. **Password Security**

1.3.1. **Organization Access Policy** – Whether the organization has a well-documented policy that provides for a password policy as well as access control policy for the exchange provided terminals.

1.3.2. **Authentication Capability** – Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.

1.3.3. **Password Best Practices** – Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.

1.4. **Session Management**

1.4.1. **Session Authentication** – Whether the system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session

authentication mechanisms like SSL etc.

1.4.2. **Session Security** – Whether there is availability of an end-to-end encryption for all data exchanged between client and broker systems. or other means of ensuring session security.

1.4.3. **Inactive Session** – Whether the system allows for automatic trading session logout after a system defined period of inactivity.

1.4.4. **Log Management** – Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.

1.5. **Network Integrity**

1.5.1. **Seamless connectivity** – Whether stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.

1.5.2. **Network Architecture** – Whether the web server is separate from the Application and Database Server.

1.5.3. **Firewall Configuration** – Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.

1.6. **Access Controls**

1.6.1. **Access to server rooms** – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.

1.6.2. **Additional Access controls** – Whether the system provides for any authentication mechanism to access to various components of the exchange provided terminals. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate

1.7. **Backup and Recovery**

1.7.1. **Backup and Recovery Policy** – Whether the organization has a well documented policy on periodic backup of data generated from the broking operations.

1.7.2. **Log generation and data consistency** - Whether backup logs are maintained and backup data is tested for consistency.

1.7.3. **System Redundancy** – Whether there are appropriate backups in case of failures of any critical system components.

1.8. **BCP/DR (Only applicable for Stock Brokers having BCP / DR site)**

1.8.1. **BCP / DR Policy** – Whether the stock broker has a well documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response procedures.

1.8.2. **Alternate channel of communication** – Whether the stock broker has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).

1.8.3. **High Availability** – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/DR policy.

1.8.4. **Connectivity with other FMIs** – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.

1.9. **Segregation of Data and Processing facilities** – The system auditor should check and comment on the segregation of data and processing facilities at the stock broker in case the stock broker is also running other business.

1.10. **Back office data**

1.10.1. **Data consistency** – The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the Stock Exchanges through online data view / download provided by exchanges to members.

1.10.2. **Trail Logs** – The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

1.11. **IT Infrastructure Management** (including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))

1.11.1. **IT Governance and Policy** – The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is

periodically assessed.

1.11.2. **IT Infrastructure Planning** – The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.

1.11.3. **IT Infrastructure Availability (SLA Parameters)** – The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm.

1.11.4. **IT Performance Monitoring (SLA Monitoring)** – The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.

1.12. **Exchange specific exceptional reports** – The additional checks recommended by a particular exchange need to be looked into and commented upon by the system auditor over and above the ToR of the system audit.

**Annexure-4**

## 2. ToR for Type II Broker

The system auditor shall at the minimum cover the following areas:

2.1. **System controls and capabilities (CTCL / IML terminals and servers)**

2.1.1. **Order Tracking** – The system auditor should verify system process and controls at CTCL / IML terminals and CTCL/ IML servers covering order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of current order/outstanding orders and trade confirmation.

2.1.2. **Order Status/ Capture** – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity, etc.

2.1.3. **Rejection of orders** – Whether system has capability to reject orders which do not go through order level validation at CTCL servers and at the servers of respective Stock Exchanges.

2.1.4. **Communication of Trade Confirmation** / Order Status – Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.

2.1.5. **Client ID Verification** – Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.

2.1.6. **Order type distinguishing capability** – Whether system has capability to distinguish the orders originating from (CTCL or IML) / IBT/ DMA / STWT.

2.2. **Software Change Management** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

2.2.1. Processing / approval methodology of new feature request or patches.

2.2.2. Fault reporting / tracking mechanism and process for resolution.

2.2.3. Testing of new releases / patches / modified software / bug fixes.

2.2.4. Version control- History, Change Management process, approval etc.

2.2.5. Development / Test / Production environment segregation.

2.2.6. New release in production – promotion, release note approvals.

2.2.7. Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.

2.2.8. User Awareness.

The system auditor should check whether critical changes made to the (CTCL or IML) / IBT / DMA / STWT/ SOR are well documented and communicated to the Stock Exchange.

2.3. **Risk Management System (RMS)**

2.3.1. **Online risk management capability** – The system auditor should check whether system of online risk management including upfront real-time risk management, is in place for all orders placed through (CTCL or IML) / IBT / DMA / STWT.

2.3.2. **Trading Limits** – Whether a system of pre-defined limits /checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc., are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.

2.3.3. **Order Alerts and Reports** – Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to margin requirements, payments and delivery obligations.

2.3.4. **Order Review** – Whether the system has capability to facilitate review of such orders that were not validated by the system.

2.3.5. **Back testing for effectiveness of RMS** – Whether system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.

2.3.6. **Log Management** – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of

changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

2.4. **Smart order routing (SOR)** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

2.4.1. **Best Execution Policy** – System adheres to the Best Execution Policy while routing the orders to the exchange.

2.4.2. **Destination Neutral** – The system routes orders to the recognized Stock Exchanges in a neutral manner.

2.4.3. **Class Neutral** – The system provides for SOR for all classes of investors.

2.4.4. **Confidentiality** - The system does not release orders to venues other than the recognized Stock Exchange.

2.4.5. **Opt–out** – The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR.

2.4.6. **Time stamped market information** – The system is capable of receiving time stamped market prices from recognized Stock Exchanges from which the member is authorized to avail SOR facility.

2.4.7. **Audit Trail** - Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.

2.4.8. **Server Location** – The system auditor should check whether the order routing server is located in India.

2.4.9. **Alternate Mode** - The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility.

2.5. **Password Security**

2.5.1. **Organization Access Policy** – Whether organization has a well-documented policy that provides for a password policy as well as access control policy for exchange provided terminals and for API based terminals.

2.5.2. **Authentication Capability** – Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication of orders originating from

Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.

2.5.3. **Password Best Practices** – Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.

2.6. **Session Management**

2.6.1. **Session Authentication** – Whether system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.

2.6.2. **Session Security** – Whether there is availability of an end-to-end encryption for all data exchanged between client and broker systems or other means of ensuring session security. Whether session login details are stored on the devices used for IBT and STWT.

2.6.3. **Inactive Session** – Whether the system allows for automatic trading session logout after a system defined period of inactivity.

2.6.4. **Log Management** – Whether the system generates and maintains logs of Number of users, activity logs, system logs, Number of active clients.

2.7. **Database Security**

2.7.1. **Access** – Whether the system allows CTCL or IML database access only to authorized users / applications.

2.7.2. **Controls** – Whether the CTCL or IML database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.

2.8. **Network Integrity**

2.8.1. **Seamless connectivity** – Whether the stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.

2.8.2. **Network Architecture** – Whether the web server is separate from the Application and Database Server.

2.8.3. **Firewall Configuration** – Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.

2.9. **Access Controls**

2.9.1. **Access to server rooms** – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.

2.9.2. **Additional Access controls** – Whether the system provides for two factor authentication mechanism to access to various CTCL or IML components. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.

2.10. **Backup and Recovery**

2.10.1. **Backup and Recovery Policy** – Whether the organization has a well-documented policy on periodic backup of data generated from the broking operations.

2.10.2. **Log generation and data consistency** - Whether backup logs are maintained and backup data is tested for consistency.

2.10.3. **System Redundancy** – Whether there are appropriate backups in case of failures of any critical system components.

2.11. **BCP/DR** (Only applicable for Stock Brokers having BCP / DR site)

2.11.1. **BCP / DR Policy** – Whether the stock broker has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response procedures.

2.11.2. **Alternate channel of communication** – Whether the stock broker has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).

2.11.3. **High Availability** – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/ DR policy.

2.11.4. **Connectivity with other FMIs** – The system auditor should check whether there is an alternative medium to communicate with Stock

Exchanges and other FMIs.

2.12. **Segregation of Data and Processing facilities** – The system auditor should check and comment on the segregation of data and processing facilities at the stock broker in case the stock broker is also running other business.

2.13. **Back office data**

2.13.1. **Data consistency** – The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the Stock Exchanges through online data view / download provided by exchanges to members.

2.13.2. **Trail Logs** – The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

2.14. **User Management**

2.14.1. **User Management Policy** – The system auditor should check whether the stock broker has a well-documented policy that provides for user management and the user management policy explicitly defines user, database and application Access Matrix.

2.14.2. **Access to Authorized users** – The system auditor should check whether the system allows access only to the authorized users of the CTCL or IML System. Whether there is a proper documentation of the authorized users in the form of User Application approval, copies of User Qualification and other necessary documents.

2.14.3. **User Creation / Deletion** – The system auditor should check whether new user's ids were created / deleted as per CTCL or IML guidelines of the exchanges and whether the user ids are unique in nature.

2.14.4. **User Disablement** – The system auditor should check whether non-complaint users are disabled and appropriate logs (such as event log and trade logs of the user) are maintained.

2.15. **IT Infrastructure Management** (including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))

2.15.1. **IT Governance and Policy** – The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist

and are regularly reviewed and updated. Compliance with these policies is periodically assessed.

2.15.2. **IT Infrastructure Planning** – The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.

2.15.3. **IT Infrastructure Availability (SLA Parameters)** – The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm.

2.15.4. **IT Performance Monitoring (SLA Monitoring)** – The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.

2.16. **Exchange specific exceptional reports** – The additional checks recommended by a particular exchange need to be looked into and commented upon by the System Auditor over and above the ToR of the System audit.

2.17. **Software Testing Procedures** - The system auditor should check whether the stock broker has complied with the guidelines and instructions of SEBI / Stock Exchanges with regard to testing of software and new patches, including the following:

2.17.1. **Test Procedure Review** – The system auditor should evaluate whether the procedures for system and software testing were proper and adequate.

2.17.2. **Documentation** – The system auditor should verify whether the documentation related to testing procedures, test data, and resulting output were adequate and follow the organization's standards.

2.17.3. **Test Cases** – The system auditor should review the internal test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange and SEBI.

**Annexure-5**

**3. ToR for Type III Broker**

The system auditor shall at the minimum cover the following areas:

3.1. **System controls and capabilities (CTCL/IML Terminals and servers)**

3.1.1. **Order Tracking** – The system auditor should verify system process and controls at CTCL / IML terminals and CTCL/ IML servers covering order entry, capturing IP address of order entry, modification / deletion of orders, status of current order/outstanding orders and trade confirmation.

3.1.2. **Order Status/ Capture** – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.

3.1.3. **Rejection of orders** – Whether the system has capability to reject orders which do not go through order level validation at CTCL servers and at the servers of respective exchanges.

3.1.4. **Communication of Trade Confirmation / Order Status** – Whether the system has capability to timely communicate to client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.

3.1.5. **Client ID Verification** – Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.

3.1.6. **Order type distinguishing capability** – Whether the system has capability to distinguish the orders originating from (CTCL or IML) / IBT / DMA / STWT / SOR / Algorithmic Trading.

3.2. **Software Change Management** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

3.2.1. Processing / approval methodology of new feature request or patches.

3.2.2. Fault reporting / tracking mechanism and process for resolution.

3.2.3. Testing of new releases / patches / modified software / bug fixes.

3.2.4. Version control- History, Change Management process, approval etc.

3.2.5. Development / Test / Production environment segregation.

3.2.6. New release in production – promotion, release note approvals.

3.2.7. Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.

3.2.8. User Awareness.

The system auditor should check whether critical changes made to the (CTCL or IML) / IBT / DMA / STWT/ SOR are well documented and communicated to the Stock Exchange.

3.3. **Risk Management System (RMS)**

3.3.1. **Online risk management capability** – The system auditor should check whether the online risk management including upfront real-time risk management, is in place for all orders placed through (CTCL or IML) / IBT/ DMA / SOR / STWT / Algorithmic Trading.

3.3.2. **Trading Limits** – Whether a system of pre-defined limits / checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc., are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.

3.3.3. **Order Alerts and Reports** – Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to margin requirements, payments and delivery obligations.

3.3.4. **Order Review** – Whether the system has capability to facilitate review of such orders that were not validated by the system.

3.3.5. **Back testing for effectiveness of RMS** – Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits should be captured by the system, documented and corrective steps taken.

3.3.6. **Log Management** – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether

the system allows only authorized users to set the risk parameter in the RMS.

3.4. **Smart order routing (SOR)** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

3.4.1. **Best Execution Policy** – System adheres to the Best Execution Policy while routing the orders to the exchange.

3.4.2. **Destination Neutral** – The system routes orders to the recognized Stock Exchanges in a neutral manner.

3.4.3. **Class Neutral** – The system provides for SOR for all classes of investors.

3.4.4. **Confidentiality** - The system does not release orders to venues other than the recognized Stock Exchange.

**3.4.5. Opt–out –** The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR**.**

3.4.6. **Time stamped market information** – The system is capable of receiving time stamped market prices from recognized Stock Exchanges from which the member is authorized to avail SOR facility.

3.4.7. **Audit Trail** - Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.

3.4.8. **Server Location** – The system auditor should check whether the order routing server is located in India.

3.4.9. **Alternate Mode** - The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility.

3.5. **Algorithmic Trading -** The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

**3.5.1. Change Management –** Whether any changes (modification/addition) to the approved algos were informed to and approved by Stock Exchange. The inclusion / removal of different versions of algos should be well documented.

3.5.2. **Online Risk Management capability** - The CTCL or IML server should have capacity to monitor orders / trades routed through algo trading and

have online risk management for all orders through Algorithmic trading and ensure that Price Check, Quantity Check, Order Value Check, Cumulative Open Order Value Check are in place.

3.5.3. **Risk Parameters Controls** – The system should allow only authorized users to set the risk parameter. The System should also maintain a log of all the risk parameter changes made.

3.5.4. **Information / Data Feed** – The auditor should comment on the various sources of information / data for the algo and on the likely impact (run away /loop situation) of the failure one or more sources to provide timely feed to the algorithm. The system auditor should verify that the algo automatically stops further processing in the absence of data feed.

3.5.5. **Check for preventing loop or runaway situations** – The system auditor should check whether the brokers have real time monitoring systems to identify and shutdown/stop the algorithms which have not behaved as expected.

3.5.6. **Algo / Co-location facility Sub-letting** – The system auditor should verify if the algo / co-location facility has not been sub-letted to any other firms to access the exchange platform.

3.5.7. **Audit Trail** – The system auditor should check the following areas in audit trail:

a. Whether the audit trails can be established using unique identification for all algorithmic orders and comment on the same.
b. Whether the broker maintains logs of all trading activities.
c. Whether the records of control parameters, orders, traders and data emanating from trades executed through algorithmic trading are preserved/ maintained by the stock broker.
d. Whether changes to the control parameters have been made by authorized users as per the Access Matrix. The system auditor should specifically comment on the reasons and frequency for changing of such control parameters. Further, the system auditor should also comment on the possibility of such tweaking leading to run away/loop situation.
e. Whether the system captures the IP address from where the algo orders are originating.

3.5.8. **Systems and Procedures** – The system auditor should check and comment on the procedures, systems and technical capabilities of stock broker for carrying out trading through use of Algorithms. The system auditor should also identify any misuse or unauthorized access to algorithms or the system which runs these algorithms.

3.5.9. **Reporting to Stock Exchanges** – The system auditor should check whether the stock broker is informing the Stock Exchange regarding any incidents where the algos have not behaved as expected. The system auditor should also comment upon the time taken by the stock broker to inform the Stock Exchanges regarding such incidents.

3.6. **Password Security**

3.6.1. **Organization Access Policy** – The system auditor should whether the stock broker has a well documented policy that provides for a password policy as well as access control policy for exchange provided terminals and for API based terminals.

3.6.2. **Authentication Capability** – Whether the system authenticates user credentials by means of a password before allowing the user to login. Whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.

3.6.3. **Password Best Practices** – Whether there is a system should for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.

3.7. **Session Management**

3.7.1. **Session Authentication** – Whether the system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.

3.7.2. **Session Security** – Whether there is availability of an end-to-end encryption for all data exchanged between client and broker system or other means of ensuring session security. Whether session login details are stored on the devices used for IBT and STWT.

3.7.3. **Inactive Session** – Whether the system allows for automatic trading session logout after a system defined period of inactivity.

3.7.4. **Log Management** – Whether the system generates and maintains logs of number of users, activity logs, system logs, number of active clients.

3.8. **Database Security**

3.8.1. **Access** – Whether the system allows CTCL or IML database access only to authorized users / applications.

3.8.2. **Controls** – Whether the CTCL or IML database server is hosted on a secure platform, with username and password stored in an encrypted form using strong encryption algorithms.

3.9. **Network Integrity**

3.9.1. **Seamless connectivity** – Whether the stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.

3.9.2. **Network Architecture** – Whether the web server is separate from the Application and Database Server.

3.9.3. **Firewall Configuration** – Whether appropriate firewall are present between the stock broker's trading setup and various communication links to the exchange. Whether the firewalls should be appropriately configured to ensure maximum security.

3.10. **Access Controls**

3.10.1. **Access to server rooms** – Whether adequate controls are in place for access to server rooms, proper audit trails should be maintained for the same.

3.10.2. **Additional Access controls** - Whether the system should provide for two factor authentication mechanism to access to various CTCL or IML components. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.

3.11. **Backup and Recovery**

3.11.1. **Backup and Recovery Policy** – Whether the organization has a well documented policy on periodic backup of data generated from the broking operations.

3.11.2. **Log generation and data consistency** – Whether backup logs are maintained and backup data should be tested for consistency.

3.11.3. **System Redundancy** – Whether there are appropriate backups in case of failures of any critical system components

3.12. **BCP/DR (Only applicable for Stock Brokers having BCP / DR site)**

3.12.1. **BCP / DR Policy** – Whether the stock broker has a well documented BCP / DR policy and plan. The system auditor should comment on the documented incident response procedures.

3.12.2. **Alternate channel of communication** – Whether the stock broker has provided its clients with alternative means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).

3.12.3. **High Availability** – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP / DR policy.

3.12.4. **Connectivity with other FMIs** – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.

3.13. **Segregation of Data and Processing facilities** – The system auditor should check and comment on the segregation of data and processing facilities at the stock broker in case the stock broker is also running other business.

3.14. **Back office data**

3.14.1. **Data consistency** – The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the Stock Exchanges through online data view / download provided by exchanges to members.

3.14.2. **Trail Logs** – The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

3.15. **User Management**

3.15.1. **User Management Policy** – The system auditor should verify whether the stock broker has a well documented policy that provides for user management and the user management policy explicitly defines user, database and application access matrix.

3.15.2. **Access to Authorized users** – The system auditor should verify whether the system allows access only to the authorized users of the CTCL or IML system. Whether there is a proper documentation of the authorized users in the form of user application approval, copies of user qualification and other necessary documents.

3.15.3. **User Creation / Deletion** – The system auditor should verify whether new users ids should be created / deleted as per CTCL or IML guidelines of the exchanges and whether the user ids are unique in nature.

3.15.4. **User Disablement** – The system auditor should verify whether non-complaint users are disabled and appropriate logs such as event log and trade logs of the user should be maintained.

3.16. **IT Infrastructure Management** (including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))

3.16.1. **IT Governance and Policy** – The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is periodically assessed.

3.16.2. **IT Infrastructure Planning** – The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.

3.16.3. **IT Infrastructure Availability (SLA Parameters)** – The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm.

3.16.4. **IT Performance Monitoring (SLA Monitoring)** – The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.

3.17. **Exchange specific exceptional reports** – The additional checks recommended by a particular exchange need to be looked into and commented upon by the system auditor over and above the ToR of the system audit.

3.18. **Software Testing Procedures** - The system auditor shall audit whether the stock broker has complied with the guidelines and instructions of SEBI / Stock

Exchanges with regard to testing of software and new patches including the following:

3.18.1. **Test Procedure Review** – The system auditor should review and evaluate the procedures for system and program testing. The system auditor should also review the adequacy of tests.

3.18.2. **Documentation** – The system auditor should review documented testing procedures, test data, and resulting output to determine if they are comprehensive and if they follow the organization's standards.

3.18.3. **Test Cases** – The system auditor should review the test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange and various SEBI Circulars.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

**Annexure-6**

**Executive Summary Reporting Format**

**For Preliminary Audit**

| Audit Date | Observation | Description of Finding | Department | Status / Nature of Findings | Risk Ratings of Findings | Audit TOR Clause | Audited by | Root cause Analysis | Impact Analysis | Suggested Corrective action | Deadline for the Corrective Action | Verified By | Closing date |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

**Description of relevant Table heads**

1. **Audit Date –** This indicates the date of conducting the audit
2. **Description of Findings/ Observations –** Description of the findings in sufficient detail, referencing any accompanying evidence (e.g. copies of procedures, interview notes, screen shots etc.)
3. **Status/ Nature of Findings -** the category can be specified for example:
   a. Non Compliant
   b. Work In progress
   c. Observation
   d. Suggestion

4. **Risk Rating of Findings –** A rating has to been given for each of the observations based on their impact and severity to reflect the risk exposure, as well as the suggested priority for action.

| Rating | Description |
|---|---|
| **HIGH** | Weakness in control those represent exposure to the organization or risks that could lead to instances of non-compliance with the requirements of TORs. These risks need to be addressed with utmost priority. |
| **MEDIUM** | Potential weakness in controls, which could develop into an exposure or issues that represent areas of concern and may impact internal controls. These should be addressed reasonably promptly. |
| **LOW** | Potential weaknesses in controls, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls. |

5. **Audit TOR Clause** – The TOR clause corresponding to this observation.
6. **Root cause Analysis** –A detailed analysis on the cause of the nonconformity
7. **Impact Analysis** – An analysis of the likely impact on the operations/ activity of the organization.
8. **Suggested Corrective Action** –The action to be taken by the broker to correct the nonconformity.

**For Follow on / Follow up System Audit**

| Preliminary Audit Date | S. No. | Preliminary Observation Number | Preliminary Status | Preliminary Corrective Action | Current Finding | Current Status | Revised Corrective Action | Deadline for the Revised Corrective Action | Verified By | Closing date |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

**Description of relevant Table heads**

1. **Preliminary Status –** The original finding as per the preliminary System Audit Report.
2. **Preliminary Corrective Action –** The original corrective action as prescribed in the preliminary System Audit report.
3. **Current Finding –** The current finding w.r.t. the issue.
4. **Current Status –** Current status of the issue viz Compliant, Non-Compliant, Work In Progress (WIP).
5. **Revised Corrective Action –** The revised corrective action prescribed w.r.t. the Non-Compliant / WIP issues.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

**Annexure-7**

# ACCOUNT OPENING KIT

## INDEX OF DOCUMENTS

| S. No. | Name of the Document | Brief Significance of the Document | Page No |
|---|---|---|---|
| **MANDATORY DOCUMENTS AS PRESCRIBED BY SEBI & EXCHANGES** | | | |
| 1 | Account Opening Form | A. KYC form - Document captures the basic information | |
| | | B. Document captures the additional information about the constituent relevant to trading account | |
| 2 | Rights and Obligations | Document stating the Rights & Obligations of stock broker/trading memberand client for trading on exchanges (including additional rights & obligations in case of internet/wireless technology based | |
| 3 | Risk Disclosure Document (RDD) | Document detailing risks associated with dealing in the | |
| 4 | Guidance note | Document detailing do's and don'ts for trading on exchange, | |
| 5 | Policies and Procedures | Document describing significant policies and procedures of | |
| 6 | Tariff sheet | Document detailing the rate/amount of brokerage and other charges levied on the client for trading on the stock | |
| **VOLUNTARY DOCUMENTS AS PROVIDED BY THE STOCK BROKER** | | | |
| 7 | Demat Debit and Pledge Instruction' (DDPI) | Document seeking authorization by client to the stock broker, to access the demat account of the client for specified purposes only. | |
| 8 | | | |

Name of stock broker/trading member/clearing member: ----------
---------- SEBI Registration No. and date: ----------
---------- Registered office address: ----------
---------- Ph: ---------- Fax: ---------- Website: --------
---------- Correspondence office address: ----------
---------- Ph: ---------- Fax: ----------
---------- Website: ---------- *Compliance officer*

*name, phone no. & email id: ---------- CEO name, phone no. & email id: ----------*

*For any grievance/dispute please contact stock broker (name) at the above address or email id- xxx@email.com and Phone no. 91-XXXXXXXXXX. In case not satisfied with the response, please contact the concerned exchange(s) at xyz@email.com and Phone no. 91-XXXXXXXXXX.*

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-8

### *TRADING ACCOUNT RELATED DETAILS*

***For Individuals & Non-individuals***

**A. BANK ACCOUNT(S) DETAILS**

| Bank Name | Branch address | Bank account no. | Account Type: Saving/Current/ Others-In case of NRI/NRE/NRO | MICR Number | IFSC code |
|---|---|---|---|---|---|
| | | | | | |

**B. DEPOSITORY ACCOUNT(S) DETAILS**

| Depository Participant Name | Depository Name (NSDL/CDSL) | Beneficiary name | DP ID | Beneficiary ID (BO ID) |
|---|---|---|---|---|
| | | | | |

**C. TRADING PREFERENCES**

**Please sign in the relevant boxes where you wish to trade. The segment not chosen should be struck off by the client.*

| **Exchanges** | **Segments** | | | |
|---|---|---|---|---|
| Name of the Exchange -1 | Cash | | Currency Derivative | |
| | F&O | | Name of other Segment s, if any | |
| Name of the Exchange -2 | Name of the Segments -1, 2... | | | |

*# If, in future, the client wants to trade on any new segment/new exchange, separate authorization/letter should be taken from the client by the stock broker.*

**D. OTHER DETAILS (*For Individuals*)**

1. **Gross Annual Income Details (please specify):** Income Range per annum: Below Rs 1 Lac / 1-5 Lac /5-10 Lac / 10-25 Lac / >25 Lacs **or**
   **Net-worth** as on (date)…… (----------) (Net worth should not be older than 1 year)
2. **Occupation (please tick any one and give brief details):** Private Sector/ Public Sector/ Government Service/Business/ Professional/ Agriculturist/ Retired/ Housewife/ Student/ Others _
3. **Please tick, if applicable:** Politically Exposed Person (PEP)/ Related to a Politically Exposed Person (PEP)
4. **Any other information**: ____

**E. OTHER DETAILS (*For Non-Individuals*)**

1. **Gross Annual Income Details (please specify):** Income Range per annum: Below Rs 1 Lac / 1-5 Lac /5-10 Lac / 10-25 Lac / 25 Lacs-1 crore / > 1 crore
2. **Net-worth** as on (date) …… (dd/mm/yyyy): (Net worth should not be older than 1 year)
3. **Name, PAN, residential address and photographs of Promoters/Partners/Karta/Trustees and whole time directors:** _____
4. **DIN/UID of Promoters/Partners/Karta and whole time directors:**
5. **Please tick, if applicable, for any of your authorized signatories/Promoters/Partners/Karta/Trustees/whole time directors: Politically Exposed Person (PEP)/ Related to a Politically Exposed Person (PEP)**

6. **Any other information: ____**

**F. PAST ACTIONS**

- Details of any action/proceedings initiated/pending/ taken by SEBI/ Stock exchange/any other authority against the applicant/constituent or its Partners/promoters/whole time directors/authorized persons in charge of dealing in securities during the last 3 years: ……

**G. DEALINGS THROUGH OTHER STOCK BROKERS**

- Whether dealing with any other stock broker (if case dealing with multiple stock brokers, provide details of all)
  Name of stock broker:……:……..
  Client Code: ……Exchange:……
  Details of disputes/dues pending from/to such stock broker: ……

**H. ADDITIONAL DETAILS**

- Whether you wish to receive physical contract note or Electronic Contract Note (ECN) (please specify): ……
  Specify your Email id, if applicable: ……...
- Whether you wish to avail of the facility of internet trading/ wireless technology (please specify): ……
- Number of years of Investment/Trading Experience: ……
- In case of non-individuals, name, designation, PAN, UID, signature, residential address and photographs of persons authorized to deal in securities on behalf of company/firm/others: ……
- Any other information: ……..

**I. INTRODUCER DETAILS (optional)**

Name of the Introducer: ……
(Surname) (Name) (Middle Name)
Status of the Introducer: Remisier/Authorized Person/Existing Client/Others, please specify……
Address and phone no. of the Introducer: …… Signature of the Introducer: ……

**J. NOMINATION DETAILS (for individuals only)**

**I/We wish to nominate** **I/We do not wish to nominate**

Name of the Nominee: …… Relationship with the Nominee: ……
PAN of Nominee: ……... Date of Birth of Nominee: ……
Address and phone no. of the Nominee: ……

**If Nominee is a minor, details of guardian:**

Name of guardian: …… Address and phone no. of Guardian: ……..
Signature of guardian ……

**WITNESSES** (Only applicable in case the account holder has made nomination)

Name ---------- Name ----------
Signature ---------- Signature ----------
Address ---------- Address ----------

## DECLARATION

1. I/We hereby declare that the details furnished above are true and correct to the best of my/our knowledge and belief and I/we undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I am/we are aware that I/we may be held liable for it.

2. I/We confirm having read/been explained and understood the contents of the document on policy and procedures of the stock broker and the tariff sheet.

3. I/We further confirm having read and understood the contents of the 'Rights and Obligations' document(s) and 'Risk Disclosure Document'. I/We do hereby agree to be bound by such provisions as outlined in these documents. I/We have also been informed that the standard set of documents has been displayed for Information on stock broker's designated website, if any.

**Place** ----------
**Date** ----------

(----------)
**Signature of Client/ (all) Authorized Signatory (ies)**

---

## FOR OFFICE USE ONLY

UCC Code allotted to the Client: ----------

| | Documents verified with Originals | Client Interviewed By | In-Person Verification done by |
|---|---|---|---|
| Name of the Employee | | | |
| Employee Code | | | |
| Designation of the employee | | | |
| Date | | | |
| Signature | | | |

*I / We undertake that we have made the client aware of 'Policy and Procedures', tariff sheet and all the non-mandatory documents. I/We have also made the client aware of 'Rights and Obligations' document (s), RDD and Guidance Note. I/We have given/sent him a copy of all the KYC documents. I/We undertake that any change in the 'Policy and Procedures', tariff sheet and all the non-mandatory documents would be duly intimated to the clients. I/We also undertake that any change in the 'Rights and Obligations' and RDD would be made available on my/our website, if any, for the information of the clients.*

**……..**
**Signature of the Authorised Signatory**

**Date …….**

**Seal/Stamp of the stock broker**

## INSTRUCTIONS/ CHECK LIST

1. Additional documents in case of trading in derivatives segments - illustrative list:

| | |
|---|---|
| Copy of ITR Acknowledgement | Copy of Annual Accounts |
| In case of salary income - Salary Slip, Copy of Form 16 | Net worth certificate |
| Copy of demat account holding statement. | Bank account statement for last 6 months |
| Any other relevant documents substantiating ownership of assets. | Self declaration with relevant supporting documents. |

**In respect of other clients, documents as per risk management policy of the stock broker need to be provided by the client from time to time.*

2. Copy of cancelled cheque leaf/ pass book/bank statement specifying name of the constituent, MICR Code or/and IFSC Code of the bank should be submitted.

3. Demat master or recent holding statement issued by DP bearing name of the client.

4. For individuals:
    a. Stock broker has an option of doing 'in-person' verification through web camera at the branch office of the stock broker
    b. In case of non-resident clients, employees at the stock broker's local office, overseas can do in-person' verification. Further, considering the infeasibility of carrying out 'In-person' verification of the non-resident clients by the stock broker's staff, attestation of KYC documents by Notary Public, Court, Magistrate, Judge, Local Banker, Indian Embassy / Consulate General in the country where the client resides may be permitted.

5. For non-individuals:
    a. Form need to be initialized by all the authorized signatories.
    b. Copy of Board Resolution or declaration (on the letterhead) naming the persons authorized to deal in securities on behalf of company/firm/others and their specimen signatures.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-9

### RIGHTS AND OBLIGATIONS OF STOCK BROKERS AND CLIENTS
***as prescribed by SEBI and Stock Exchanges***

1. The client shall invest/trade in those securities/contracts/other instruments admitted to dealings on the Exchanges as defined in the Rules, Byelaws and Regulations of Exchanges/ Securities and Exchange Board of India (SEBI) and circulars/notices issued there under from time to time.

2. The stock broker, and the client shall be bound by all the Rules, Byelaws and Regulations of the Exchange and circulars/notices issued there under and Rules and Regulations of SEBI and relevant notifications of Government authorities as may be in force from time to time.

3. The client shall satisfy itself of the capacity of the stock broker to deal in securities and/or deal in derivatives contracts and wishes to execute its orders through the stock broker and the client shall from time to time continue to satisfy itself of such capability of the stock broker before executing orders through the stock broker.

4. The stock broker shall continuously satisfy itself about the genuineness and financial soundness of the client and investment objectives relevant to the services to be provided.

5. The stock broker shall take steps to make the client aware of the precise nature of the Stock broker's liability for business to be conducted, including any limitations, the liability and the capacity in which the stock broker acts.

**CLIENT INFORMATION**

6. The client shall furnish all such details in full as are required by the stock broker in "Account Opening Form" with supporting details, made mandatory by stock exchanges/SEBI from time to time.

7. The client shall familiarize himself with all the mandatory provisions in the Account Opening documents. Any additional clauses or documents specified by the stock broker shall be non-mandatory, as per terms & conditions accepted by the client.

8. The client shall immediately notify the stock broker in writing if there is any change in the information in the 'account opening form' as provided at the time of account opening and thereafter; including the information on winding up petition/insolvency petition or any litigation which may have material bearing on his capacity. The client shall provide/update the financial information to the stock broker on a periodic basis.

9. The stock broker shall maintain all the details of the client as mentioned in the account opening form or any other information pertaining to the client, confidentially and that they shall not disclose the same to any person/authority except as required under any law/regulatory requirements. Provided however that the stock broker may so disclose information about his client to any person or authority with the express permission of the client.

**MARGINS**

10. The client shall pay applicable initial margins, withholding margins, special margins or such other

margins as are considered necessary by the stock broker or the Exchange or as may be directed by SEBI from time to time as applicable to the segment(s) in which the client trades. The stock broker is permitted in its sole and absolute discretion to collect additional margins (even though not required by the Exchange, Clearing House/Clearing Corporation or SEBI) and the client shall be obliged to pay such margins within the stipulated time.

11. The client understands that payment of margins by the client does not necessarily imply complete satisfaction of all dues. In spite of consistently having paid margins, the client may, on the settlement of its trade, be obliged to pay (or entitled to receive) such further sums as the contract may dictate/require.

**TRANSACTIONS AND SETTLEMENTS**

12. The client shall give any order for buy or sell of a security/derivatives contract in writing or in such form or manner, as may be mutually agreed between the client and the stock broker. The stock broker shall ensure to place orders and execute the trades of the client, only in the Unique Client Code assigned to that client.

13. The stock broker shall inform the client and keep him apprised about trading/settlement cycles, delivery/payment schedules, any changes therein from time to time, and it shall be the responsibility in turn of the client to comply with such schedules/procedures of the relevant stock exchange where the trade is executed.

14. The stock broker shall ensure that the money/securities deposited by the client shall be kept in a separate account, distinct from his/its own account or account of any other client and shall not be used by the stock broker for himself/itself or for any other client or for any purpose other than the purposes mentioned in Rules, Regulations, circulars, notices, guidelines of SEBI and/or Rules, Regulations, Bye-laws, circulars and notices of Exchange.

15. Where the Exchange(s) cancels trade(s) suo moto all such trades including the trade/s done on behalf of the client shall ipso facto stand cancelled, stock broker shall be entitled to cancel the respective contract(s) with client(s).

16. The transactions executed on the Exchange are subject to Rules, Byelaws and Regulations and circulars/notices issued thereunder of the Exchanges where the trade is executed and all parties to such trade shall have submitted to the jurisdiction of such court as may be specified by the Byelaws and Regulations of the Exchanges where the trade is executed for the purpose of giving effect to the provisions of the Rules, Byelaws and Regulations of the Exchanges and the circulars/notices issued thereunder.

**BROKERAGE**

17. The Client shall pay to the stock broker brokerage and statutory levies as are prevailing from time to time and as they apply to the Client's account, transactions and to the services that stock broker renders to the Client. The stock broker shall not charge brokerage more than the maximum brokerage permissible as per the rules, regulations and bye-laws of the relevant stock exchanges and/or rules and regulations of SEBI.

**LIQUIDATION AND CLOSE OUT OF POSITION**

18. 1Without prejudice to the stock broker's other rights (including the right to refer a matter to arbitration), the client understands that the stock broker shall be entitled to liquidate/close out all or any of the client's

positions for non- payment of margins or other amounts, outstanding debts, etc. and adjust the proceeds of such liquidation/close out, if any, against the client's liabilities/obligations. Any and all losses and financial charges on account of such liquidation/closing-out shall be charged to and borne by the client.

19. In the event of death or insolvency of the client or his/its otherwise becoming incapable of receiving and paying for or delivering or transferring securities which the client has ordered to be bought or sold, stock broker may close out the transaction of the client and claim losses, if any, against the estate of the client. The client or his nominees, successors, heirs and assignee shall be entitled to any surplus which may result there from. The client shall note that transfer of funds/securities in favor of a Nominee shall be valid discharge by the stock broker against the legal heir.
    The stock broker shall bring to the notice of the relevant Exchange the information about default in payment/delivery and related aspects by a client. In case where defaulting client is a corporate Entity/partnership/proprietary firm or any other artificial legal entity, then the name(s) of Director(s)/Promoter(s)/Partner(s)/Proprietor as the case may be, shall also be communicated by the stock broker to the relevant Exchange(s).

**DISPUTE RESOLUTION**

20. The stock broker shall provide the client with the relevant contact details of the concerned Exchanges and SEBI.

21. The stock broker shall co-operate in redressing grievances of the client in respect of all transactions routed through it and in removing objections for bad delivery of shares, rectification of bad delivery, etc.

22. The client and the stock broker shall refer any claims and/or disputes with respect to deposits, margin money, etc., to arbitration as per the Rules, Byelaws and Regulations of the Exchanges where the trade is executed and circulars/notices issued thereunder as may be in force from time to time.

23. The stock broker shall ensure faster settlement of any arbitration proceedings arising out of the transactions entered into between him vis-à-vis the client and he shall be liable to implement the arbitration awards made in such proceedings.

24. The client/stock-broker understands that the instructions issued by an authorized representative for dispute resolution, if any, of the client/stock-broker shall be binding on the client/stock-broker in accordance with the letter authorizing the said representative to deal on behalf of the said client/stock-broker.

**TERMINATION OF RELATIONSHIP**

25. This relationship between the stock broker and the client shall be terminated; if the stock broker for any reason ceases to be a member of the stock exchange including cessation of membership by reason of the stock broker's default, death, resignation or expulsion or if the certificate is cancelled by the Board.

26. The stock broker and the client shall be entitled to terminate the relationship between them without giving any reasons to the other party, after giving notice in writing of not less than one month to the other parties. Notwithstanding any such termination, all rights, liabilities and obligations of the parties arising out of or in respect of transactions entered into prior to the termination of this relationship 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.

**ADDITIONAL RIGHTS AND OBLIGATIONS**

27. The stock broker shall ensure due protection to the client regarding client's rights to dividends, rights or bonus shares, etc. in respect of transactions routed through it and it shall not do anything which is likely to harm the interest of the client with whom and for whom they may have had transactions in securities.
28. The stock broker and client shall reconcile and settle their accounts from time to time as per the Rules, Regulations, Bye Laws, Circulars, Notices and Guidelines issued by SEBI and the relevant Exchanges where the trade is executed.
29. The stock broker shall issue a contract note to his constituents for trades executed in such format as may be prescribed by the Exchange from time to time containing records of all transactions including details of order number, trade number, trade time, trade price, trade quantity, details of the derivatives contract, client code, brokerage, all charges levied etc. and with all other relevant details as required therein to be filled in and issued in such manner and within such time as prescribed by the Exchange. The stock broker shall send contract notes to the investors within one working day of the execution of the trades in hard copy and/or in electronic form using digital signature.

30. The stock broker shall make pay out of funds or delivery of securities, as the case may be, to the Client within one working day of receipt of the payout from the relevant Exchange where the trade is executed unless otherwise specified by the client and subject to such terms and conditions as may be prescribed by the relevant Exchange from time to time where the trade is executed.

31. The stock broker shall send a complete `Statement of Accounts' for both funds and securities in respect of each of its clients in such periodicity and format within such time, as may be prescribed by the relevant Exchange, from time to time, where the trade is executed. The Statement shall also state that the client shall report errors, if any, in the Statement within such time as may be prescribed by the relevant Exchange from time to time where the trade was executed, from the receipt thereof to the Stock broker.

32. The stock broker shall send daily margin statements to the clients. Daily Margin statement should include, inter- alia, details of collateral deposited, collateral utilized and collateral status (available balance/due from client) with break up in terms of cash, Fixed Deposit Receipts (FDRs), Bank Guarantee and securities.

33. The Client shall ensure that it has the required legal capacity to, and is authorized to, enter into the relationship with stock broker and is capable of performing his obligations and undertakings hereunder. All actions required to be taken to ensure compliance of all the transactions, which the Client may enter into shall be completed by the Client prior to such transaction being entered into.

34. The stock broker / stock broker and depository participant shall not directly /indirectly compel the clients to execute Power of Attorney (PoA) or Demat Debit and Pledge Instruction (DDPI) or deny services to the client if the client refuses to execute PoA or DDPI.

**ELECTRONIC CONTRACT NOTES (ECN)**

35. In case, client opts to receive the contract note in electronic form, he shall provide an appropriate e-mail id to the stock broker. The client shall communicate to the stock broker any change in the email-id through a physical letter. If the client has opted for internet trading, the request for change of email id may be made through the secured access by way of client specific user id and password.

36. The stock broker shall ensure that all ECNs sent through the e-mail shall be digitally signed, encrypted,

non-tamper able and in compliance with the provisions of the IT Act, 2000. In case, ECN is sent through e-mail as an attachment, the attached file shall also be secured with the digital signature, encrypted and non-tamperable.

37. The client shall note that non-receipt of bounced mail notification by the stock broker shall amount to delivery of the contract note at the e-mail ID of the client.

1. The stock broker shall retain ECN and acknowledgement of the e-mail in a soft and non-tamperable form in the manner prescribed by the exchange in compliance with the provisions of the IT Act, 2000 and as per the extant rules/regulations/circulars/guidelines issued by SEBI/Stock Exchanges from time to time. The proof of delivery i.e., log report generated by the system at the time of sending the contract notes shall be maintained by the stock broker for the specified period under the extant regulations of SEBI/stock exchanges. The log report shall provide the details of the contract notes that are not delivered to the client/e-mails rejected or bounced back. The stock broker shall take all possible steps to ensure receipt of notification of bounced mails by him at all times within the stipulated time period under the extant regulations of SEBI/stock exchanges.
2. The stock broker shall continue to send contract notes in the physical mode to such clients who do not opt to receive the contract notes in the electronic form. Wherever the ECNs have not been delivered to the client or has been rejected (bouncing of mails) by the e-mail ID of the client, the stock broker shall send a physical contract note to the client within the stipulated time under the extant regulations of SEBI/stock exchanges and maintain the proof of delivery of such physical contract notes.

3. In addition to the e-mail communication of the ECNs to the client, the stock broker shall simultaneously publish the ECN on his designated web-site, if any, in a secured way and enable relevant access to the clients and for this purpose, shall allot a unique user name and password to the client, with an option to the client to save the contract note electronically and/or take a print out of the same.

**LAW AND JURISDICTION**

4. In addition to the specific rights set out in this document, the stock broker and the client shall be entitled to exercise any other rights which the stock broker or the client may have under the Rules, Bye-laws and Regulations of the Exchanges in which the client chooses to trade and circulars/notices issued thereunder or Rules and Regulations of SEBI.

5. The provisions of this document shall always be subject to Government notifications, any rules, regulations, guidelines and circulars/notices issued by SEBI and Rules, Regulations and Bye laws of the relevant stock exchanges, where the trade is executed, that may be in force from time to time.

6. The stock broker and the client shall abide by any award passed by the Arbitrator(s) under the Arbitration and Conciliation Act, 1996. However, there is also a provision of appeal within the stock exchanges, if either party is not satisfied with the arbitration award.

7. Words and expressions which are used in this document but which are not defined herein shall, unless the context otherwise requires, have the same meaning as assigned thereto in the Rules, Byelaws and Regulations and circulars/notices issued thereunder of the Exchanges/SEBI.

8. All additional voluntary clauses/document added by the stock broker should not be in contravention with rules/regulations/notices/circulars of Exchanges/SEBI. Any changes in such voluntary clauses/document(s) need to be preceded by a notice of 15 days. Any changes in the rights and obligations which are specified by Exchanges/SEBI shall also be brought to the notice of the clients.

38. If the rights and obligations of the parties hereto are altered by virtue of change in Rules and regulations of SEBI or Bye-laws, Rules and Regulations of the relevant stock Exchanges where the trade is executed, such changes shall be deemed to have been incorporated herein in modification of the rights and obligations of the parties mentioned in this document.

**INTERNET & WIRELESS TECHNOLOGY BASED TRADING FACILITY PROVIDED BY STOCK BROKERS TO CLIENT**

**(All the clauses mentioned in the *'Rights and Obligations'* document(s) shall be applicable. Additionally, the clauses mentioned herein shall also be applicable.)**

1. Stock broker is eligible for providing Internet based trading (IBT) and securities trading through the use of wireless technology that shall include the use of devices such as mobile phone, laptop with data card, etc. which use Internet Protocol (IP). The stock broker shall comply with all requirements applicable to internet based trading/securities trading using wireless technology as may be specified by SEBI & the Exchanges from time to time.

2. The client is desirous of investing/trading in securities and for this purpose, the client is desirous of using either the internet based trading facility or the facility for securities trading through use of wireless technology. The Stock broker shall provide the Stock broker's IBT Service to the Client, and the Client shall avail of the Stock broker's IBT Service, on and subject to SEBI/Exchanges Provisions and the terms and conditions specified on the Stock broker's IBT Web Site provided that they are in line with the norms prescribed by Exchanges/SEBI.

3. The stock broker shall bring to the notice of client the features, risks, responsibilities, obligations and liabilities associated with securities trading through wireless technology/internet/smart order routing or any other technology should be brought to the notice of the client by the stock broker.

4. The stock broker shall make the client aware that the Stock Broker's IBT system itself generates the initial password and its password policy as stipulated in line with norms prescribed by Exchanges/SEBI.

5. The Client shall be responsible for keeping the Username and Password confidential and secure and shall be solely responsible for all orders entered and transactions done by any person whosoever through the Stock broker's IBT System using the Client's Username and/or Password whether or not such person was authorized to do so. Also the client is aware that authentication technologies and strict security measures are required for the internet trading/securities trading through wireless technology through order routed system and undertakes to ensure that the password of the client and/or his authorized representative are not revealed to any third party including employees and dealers of the stock broker

6. The Client shall immediately notify the Stock broker in writing if he forgets his password, discovers security flaw in Stock Broker's IBT System, discovers/suspects discrepancies/ unauthorized access through his username/password/account with full details of such unauthorized use, the date, the manner and the transactions effected pursuant to such unauthorized use, etc.

7. The Client is fully aware of and understands the risks associated with availing of a service for routing orders over the internet/securities trading through wireless technology and Client shall be fully liable and responsible for any and all acts done in the Client's Username/password in any manner whatsoever.

8. The stock broker shall send the order/trade confirmation through email to the client at his request. The

client is aware that the order/ trade confirmation is also provided on the web portal. In case client is trading using wireless technology, the stock broker shall send the order/trade confirmation on the device of the client.

9. The client is aware that trading over the internet involves many uncertain factors and complex hardware, software, systems, communication lines, peripherals, etc. are susceptible to interruptions and dislocations. The Stock broker and the Exchange do not make any representation or warranty that the Stock broker's IBT Service will be available to the Client at all times without any interruption.

10. The Client shall not have any claim against the Exchange or the Stock broker on account of any suspension, interruption, non-availability or malfunctioning of the Stock broker's IBT System or Service or the Exchange's service or systems or non-execution of his orders due to any link/system failure at the Client/Stock brokers/Exchange end for any reason beyond the control of the stock broker/Exchanges.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-10

**RISK DISCLOSURE DOCUMENT FOR CAPITAL MARKET AND DERIVATIVES SEGMENTS**

This document contains important information on trading in Equities/Derivatives Segments of the stock exchanges. All prospective constituents should read this document before trading in Equities/Derivatives Segments of the Exchanges.

Stock exchanges/SEBI does neither singly or jointly and expressly nor impliedly guarantee nor make any representation concerning the completeness, the adequacy or accuracy of this disclosure document nor have Stock exchanges /SEBI endorsed or passed any merits of participating in the trading segments. This brief statement does not disclose all the risks and other significant aspects of trading.

In the light of the risks involved, you should undertake transactions only if you understand the nature of the relationship into which you are entering and the extent of your exposure to risk.

You must know and appreciate that trading in Equity shares, derivatives contracts or other instruments traded on the Stock Exchange, which have varying element of risk, is generally not an appropriate avenue for someone of limited resources/limited investment and/or trading experience and low risk tolerance. You should therefore carefully consider whether such trading is suitable for you in the light of your financial condition. In case you trade on Stock exchanges and suffer adverse consequences or loss, you shall be solely responsible for the same and Stock exchanges/its Clearing Corporation and/or SEBI shall not be responsible, in any manner whatsoever, for the same and it will not be open for you to take a plea that no adequate disclosure regarding the risks involved was made or that you were not explained the full risk involved by the concerned stock broker. The constituent shall be solely responsible for the consequences and no contract can be rescinded on that account. You must acknowledge and accept that there can be no guarantee of profits or no exception from losses while executing orders for purchase and/or sale of a derivative contract being traded on Stock exchanges.

It must be clearly understood by you that your dealings on Stock exchanges through a stock broker shall be subject to your fulfilling certain formalities set out by the stock broker, which may inter alia include your filling the know your client form, reading the rights and obligations, do's and don'ts, etc., and are subject to the Rules, Byelaws and Regulations of relevant Stock exchanges, its Clearing Corporation, guidelines prescribed by SEBI and in force from time to time and Circulars as may be issued by Stock exchanges or its Clearing Corporation and in force from time to time.

Stock exchanges does not provide or purport to provide any advice and shall not be liable to any person who enters into any business relationship with any stock broker of Stock exchanges and/or any third party based on any information contained in this document. Any information contained in this document must

not be construed as business advice. No consideration to trade should be made without thoroughly understanding and reviewing the risks involved in such trading. If you are unsure, you must seek professional advice on the same.

In considering whether to trade or authorize someone to trade for you, you should be aware of or must get acquainted with the following:-

**1. BASIC RISKS:**

**1.1 Risk of Higher Volatility:**
Volatility refers to the dynamic changes in price that a security/derivatives contract undergoes when trading activity continues on the Stock Exchanges. Generally, higher the volatility of a security/derivatives contract, greater is its price swings. There may be normally greater volatility in thinly traded securities / derivatives contracts than in active securities /derivatives contracts. As a result of volatility, your order may only be partially executed or not executed at all, or the price at which your
order got executed may be substantially different from the last traded price or change substantially thereafter, resulting in notional or real losses.

**1.2 Risk of Lower Liquidity:**
Liquidity refers to the ability of market participants to buy and/or sell securities / derivatives contracts expeditiously at a competitive price and with minimal price difference. Generally, it is assumed that more the numbers of orders available in a
market, greater is the liquidity. Liquidity is important because with greater liquidity, it is easier for investors to buy and/or sell securities / derivatives contracts swiftly and with minimal price difference, and as a result, investors are more likely to pay or receive a competitive price for securities / derivatives contracts purchased or sold. There may be a risk of lower liquidity in some securities / derivatives contracts as compared to active securities / derivatives contracts. As a result, your order may only be partially executed, or may be executed with relatively greater price difference or may not be executed at all.

**1.2.1** Buying or selling securities / derivatives contracts as part of a day trading strategy may also result into losses, because in such a situation, securities / derivatives contracts may have to be sold / purchased at low / high prices, compared to the expected price levels, so as not to have any open position or obligation to deliver or receive a security / derivatives contract.

**1.3 Risk of Wider Spreads:**
Spread refers to the difference in best buy price and best sell price. It represents the differential between the price of buying a security / derivatives contract and immediately selling it or vice versa. Lower liquidity and higher volatility may result in wider than normal spreads for less liquid or illiquid securities / derivatives contracts. This in turn will hamper better price formation.

**1.4 Risk-reducing orders:**

The placing of orders (e.g., "stop loss" orders, or "limit" orders) which are intended to limit losses to certain amounts may not
be effective many a time because rapid movement in market conditions may make it impossible to execute such orders.

**1.4.1** A "market" order will be executed promptly, subject to availability of orders on opposite side, without regard to price and that, while the customer may receive a prompt execution of a "market" order, the execution may be at available prices of outstanding orders, which satisfy the order quantity, on price time priority. It may be understood that these prices may be significantly different from the last traded price or the best price in that security / derivatives contract.

**1.4.2** A "limit" order will be executed only at the "limit" price specified for the order or a better price. However, while the customer receives price protection, there is a possibility that the order may not be executed at all.

**1.4.3** A stop loss order is generally placed "away" from the current price of a stock / derivatives contract, and such order gets activated if and when the security / derivatives contract reaches, or trades through, the stop price. Sell stop orders are entered ordinarily below the current price, and buy stop orders are entered ordinarily above the current price. When the security / derivatives contract reaches the pre - determined price, or trades through such price, the stop loss order converts to a market/limit order and is executed at the limit or better. There is no assurance therefore that the limit order will be executable since a security / derivatives contract might penetrate the pre-determined price, in which case, the risk of such order not getting executed arises, just as with a regular limit order.

**1.5 Risk of News Announcements:**

News announcements that may impact the price of stock / derivatives contract may occur during trading, and when combined with lower liquidity and higher volatility, may suddenly cause an unexpected positive or negative movement in the price of the
security / contract.

**1.6 Risk of Rumors:**

Rumors about companies / currencies at times float in the market through word of mouth, newspapers, websites or news agencies, etc. The investors should be wary of and should desist from acting on rumors.

**1.7 System Risk:**

High volume trading will frequently occur at the market opening and before market close. Such high volumes may also occur at any point in the day. These may cause delays in order execution or confirmation.

**1.7.1** During periods of volatility, on account of market participants continuously modifying their order quantity or prices or placing fresh orders, there may be delays in order execution and its confirmations.

**1.7.2** Under certain market conditions, it may be difficult or impossible to liquidate a position in the market at a reasonable price or at all, when there are no outstanding orders either on the buy side or the sell side, or if trading is halted in a security / derivatives contract due to any action on account of unusual trading activity or security / derivatives contract hitting circuit filters or for any other reason.

**1.8 System/Network Congestion:**

Trading on exchanges is in electronic mode, based on satellite/leased line based communications, combination of technologies and computer systems to place and route orders. Thus, there exists a possibility of communication failure or
system problems or slow or delayed response from system or trading halt, or any such other problem/glitch whereby not being able to establish access to the trading system/network, which may be beyond control and may result in delay in processing or not processing buy or sell orders either in part or in full. You are cautioned to note that although these problems may be temporary in nature, but when you have outstanding open positions or unexecuted orders, these represent a risk because of your obligations to settle all executed transactions.

**2. As far as Derivatives segments are concerned, please note and get yourself acquainted with the following additional features:-**

**2.1 Effect of "Leverage" or "Gearing":**

In the derivatives market, the amount of margin is small relative to the value of the derivatives contract so the transactions are 'leveraged' or 'geared'. Derivatives trading, which is conducted with a relatively small amount of margin, provides the
possibility of great profit or loss in comparison with the margin amount. But transactions in derivatives carry a high degree of
risk.

You should therefore completely understand the following statements before actually trading in derivatives and also trade with caution while taking into account one's circumstances, financial resources, etc. If the prices move against you, you may lose a part of or whole margin amount in a relatively short period of time. Moreover, the loss may exceed the original margin amount.

A. Futures trading involve daily settlement of all positions. Every day the open positions are marked to market based on the closing level of the index / derivatives contract. If the contract has moved against you, you will be required to deposit the amount of loss (notional) resulting from such movement. This amount will have to be paid within a stipulated time frame, generally before commencement of trading on next day.

B. If you fail to deposit the additional amount by the deadline or if an outstanding debt occurs in your account, the stock broker may liquidate a part of or the whole position or substitute securities. In this case, you will be liable for any losses incurred due to such close-outs.

C. Under certain market conditions, an investor may find it difficult or impossible to execute transactions. For example, this situation can occur due to factors such as illiquidity i.e. when there are insufficient bids or offers or suspension of trading due to price limit or circuit breakers etc.

D. In order to maintain market stability, the following steps may be adopted: changes in the margin rate, increases in the cash margin rate or others. These new measures may also be applied to the existing open interests. In such conditions, you will be required to put up additional margins or reduce your positions.

E. You must ask your broker to provide the full details of derivatives contracts you plan to trade i.e. the contract specifications and the associated obligations.

**2.2 Currency specific risks:**

1. The profit or loss in transactions in foreign currency-denominated contracts, whether they are traded in your own or another jurisdiction, will be affected by fluctuations in currency rates where there is a need to convert from the currency denomination of the contract to another currency.

2. Under certain market conditions, you may find it difficult or impossible to liquidate a position. This can occur, for example when a currency is deregulated or fixed trading bands are widened.

3. Currency prices are highly volatile. Price movements for currencies are influenced by, among other things: changing supply-demand relationships; trade, fiscal, monetary, exchange control programs and policies of governments; foreign political and economic events and policies; changes in national and international interest rates and inflation; currency devaluation; and sentiment of the market place. None of these factors can be controlled by any individual advisor and no assurance can be given that an advisor's advice will result in profitable trades for a participating customer or that a customer will not incur losses from such events.

**2.3 Risk of Option holders:**

1. An option holder runs the risk of losing the entire amount paid for the option in a relatively short period of time. This risk reflects the nature of an option as a wasting asset which becomes worthless when it expires. An option holder who neither
sells his option in the secondary market nor exercises it prior to its expiration will necessarily lose his entire investment in the option. If the price of the underlying does not change in the anticipated direction before the option expires, to an extent

sufficient to cover the cost of the option, the investor may lose all or a significant part of his investment in the option.

2. The Exchanges may impose exercise restrictions and have absolute authority to restrict the exercise of options at certain times in specified circumstances.

**2.4 Risks of Option Writers:**

1. If the price movement of the underlying is not in the anticipated direction, the option writer runs the risks of losing substantial amount.
2. The risk of being an option writer may be reduced by the purchase of other options on the same underlying interest and
thereby assuming a spread position or by acquiring other types of hedging positions in the options markets or other markets. However, even where the writer has assumed a spread or other hedging position, the risks may still be significant. A spread position is not necessarily less risky than a simple 'long' or 'short' position.
3. Transactions that involve buying and writing multiple options in combination, or buying or writing options in combination with
buying or selling short the underlying interests, present additional risks to investors. Combination transactions, such as option spreads, are more complex than buying or writing a single option. And it should be further noted that, as in any area of investing, a complexity not well understood is, in itself, a risk factor. While this is not to suggest that combination strategies should not be considered, it is advisable, as is the case with all investments in options, to consult with someone who is experienced and knowledgeable with respect to the risks and potential rewards of combination transactions under various market circumstances.

**3. TRADING THROUGH WIRELESS TECHNOLOGY/ SMART ORDER ROUTING OR ANY OTHER TECHNOLOGY:**

Any additional provisions defining the features, risks, responsibilities, obligations and liabilities associated with securities trading through wireless technology/ smart order routing or any other technology should be brought to the notice of the client by the stock broker.

**4. GENERAL**

4.1 The term ‘constituent’ shall mean and include a client, a customer or an investor, who deals with a stock broker for the purpose of acquiring and/or selling of securities / derivatives contracts through the mechanism provided by the Exchanges.

4.2 The term ‘stock broker’ shall mean and include a stock broker, a broker or a stock broker, who has been admitted as such by the Exchanges and who holds a registration certificate from SEBI.

## Annexure-11

### GUIDANCE NOTE - DO's AND DON'Ts FOR TRADING ON THE EXCHANGE(S) FOR INVESTORS

**BEFORE YOU BEGIN TO TRADE**

1. Ensure that you deal with and through only SEBI registered intermediaries. You may check their SEBI registration certificate number from the list available on the Stock exchanges www.exchange.com and SEBI website www.sebi.gov.in.
2. Ensure that you fill the KYC form completely and strike off the blank fields in the KYC form.
3. Ensure that you have read all the mandatory documents viz. Rights and Obligations, Risk Disclosure Document, Policy and Procedure document of the stock broker.
4. Ensure to read, understand and then sign the voluntary clauses, if any, agreed between you and the stock broker. Note that the clauses as agreed between you and the stock broker cannot be changed without your consent.
5. Get a clear idea about all brokerage, commissions, fees and other charges levied by the broker on you for trading and the relevant provisions/ guidelines specified by SEBI/Stock exchanges.
6. Obtain a copy of all the documents executed by you from the stock broker free of charge.
7. In case you wish to execute Power of Attorney (POA) in favour of the Stock broker, authorizing it to operate your bank and demat account, please refer to the guidelines issued by SEBI/Exchanges in this regard.

**TRANSACTIONS AND SETTLEMENTS**

8. The stock broker may issue electronic contract notes (ECN) if specifically authorized by you in writing. You should provide your email id to the stock broker for the same. Don't opt for ECN if you are not familiar with computers.
9. Don't share your internet trading account's password with anyone.
10. Don't make any payment in cash to the stock broker.
11. Make the payments by account payee cheque in favour of the stock broker. Don't issue cheques in the name of sub- broker. Ensure that you have a documentary proof of your payment/deposit of securities with the stock broker, stating date, scrip, quantity, towards which bank/ demat account such money or securities deposited and from which bank/ demat account.
12. Note that facility of Trade Verification is available on stock exchanges' websites, where details of trade as mentioned in the contract note may be verified. Where trade details on the website do not tally with the details mentioned in the contract note, immediately get in touch with the Investors Grievance Cell of the relevant Stock exchange.
13. In case you have given specific authorization for maintaining running account, payout of funds or delivery of securities (as the case may be), may not be made to you within one working day from the receipt of payout from the Exchange. Thus, the stock broker shall maintain running account for you subject to the following conditions:
    a) Such authorization from you shall be dated, signed by you only and contains the clause that you may revoke the same at any time.
    b) The actual settlement of funds and securities shall be done by the stock broker, at least once in a calendar quarter or month, depending on your preference. While settling the account, the stock broker shall send to you a 'statement of accounts' containing an extract from the client ledger for funds and an extract from the register of securities displaying all the receipts/deliveries of funds and securities. The

statement shall also explain the retention of funds and securities and the details of the pledged shares, if any.

c) On the date of settlement, the stock broker may retain the requisite securities/funds towards outstanding obligations and may also retain the funds expected to be required to meet derivatives margin obligations for next 5 trading days, calculated in the manner specified by the exchanges. In respect of cash market transactions, the stock broker may retain entire pay-in obligation of funds and securities due from clients as on date of settlement and for next day's business, he may retain funds/securities/margin to the extent of value of transactions executed on the day of such settlement in cash market.

d) You need to bring any dispute arising from the statement of account or settlement so made to the notice of the stock broker in writing preferably within 7 (seven) working days from the date of receipt of funds/securities or statement, as the case may be. In case of dispute, refer the matter in writing to the Investors Grievance Cell of the relevant Stock exchanges without delay.

14. In case you have not opted for maintaining running account and pay-out of funds/securities is not received on the next working day of the receipt of payout from the exchanges, please refer the matter to the stock broker. In case there is dispute, ensure that you lodge a complaint in writing immediately with the Investors Grievance Cell of the relevant Stock exchange.
15. Please register your mobile number and email id with the stock broker, to receive trade confirmation alerts/ details of the transactions through SMS or email, by the end of the trading day, from the stock exchanges.

**IN CASE OF TERMINATION OF TRADING MEMBERSHIP**

16. In case, a stock broker surrenders his membership, is expelled from membership or declared a defaulter; Stock exchanges gives a public notice inviting claims relating to only the "transactions executed on the trading system" of Stock exchange, from the investors. Ensure that you lodge a claim with the relevant Stock exchanges within the stipulated period and with the supporting documents.
17. Familiarize yourself with the protection accorded to the money and/or securities you may deposit with your stock broker, particularly in the event of a default or the stock broker's insolvency or bankruptcy and the extent to which you may recover such money and/or securities may be governed by the Bye-laws and Regulations of the relevant Stock exchange
where the trade was executed and the scheme of the Investors' Protection Fund in force from time to time.

**DISPUTES/ COMPLAINTS**

18. Please note that the details of the arbitration proceedings, penal action against the brokers and investor complaints against the stock brokers are displayed on the website of the relevant Stock exchange.
19. In case your issue/problem/grievance is not being sorted out by concerned stock broker/sub-broker then you may take up the matter with the concerned Stock exchange. If you are not satisfied with the resolution of your complaint then you can escalate the matter to SEBI.
20. Note that all the stock broker/sub-brokers have been mandated by SEBI to designate an e-mail ID of the grievance redressal division/compliance officer exclusively for the purpose of registering complaints.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-12

## Nomination Form

| TM / DP Name and Address | FORM FOR NOMINATION<br>(*To be filled in by individual applying singly or jointly*) |
|---|---|
| Date D D M M Y Y Y Y | UCC/ DP ID I N Client ID |

I/We wish to make a nomination. [*As per details given below*]

**Nomination Details**

I/We wish to make a nomination and do hereby nominate the following person(s) who shall receive all the assets held in my / our account in the event of my / our death.

| | | | Details of 1st Nominee | Details of 2nd Nominee | Details of 3rd Nominee |
|---|---|---|---|---|---|
| | **Nomination can be made upto three nominees in the account.** | | | | |
| 1 | **Name of the nominee(s) (Mr./Ms.)** | | | | |
| 2 | **Share of each Nominee** | Equally<br>[If not equally, please specify percentage] | % | % | % |
| | | | *Any odd lot after division shall be transferred to the first nominee mentioned in the form.* | | |
| 3 | **Relationship With the Applicant ( If Any)** | | | | |
| 4 | **Address of Nominee(s)**<br>City / Place:<br>State & Country: | | | | |
| | | PIN Code | | | |
| 5 | **Mobile / Telephone No. of nominee(s) #** | | | | |
| 6 | **Email ID of nominee(s) #** | | | | |
| 7 | **Nominee Identification details #** [Please tick any one of following and provide details of same]<br>□ Photograph & Signature □ PAN<br>□ Aadhaar □ Saving Bank account no. □ Proof of Identity □ Demat Account ID | | | | |
| **Sr. Nos. 8-14 should be filled only if nominee(s) is a minor:** | | | | | |
| 8 | **Date of Birth {in case of minor nominee(s)}** | | | | |

| | | | | |
|---|---|---|---|---|
| **9** | **Name of Guardian (Mr./Ms.) {in case of minor nominee(s) }** | | | |
| **10** | **Address of Guardian(s)** | | | |
| | City / Place:<br>State & Country: | | | |
| | PIN Code | | | |
| **11** | **Mobile / Telephone no. of Guardian #** | | | |
| **12** | **Email ID of Guardian #** | | | |
| **13** | **Relationship of Guardian with nominee** | | | |
| **14** | **Guardian Identification details#** [Please tick any one of following and provide details of same]<br><br>□ Photograph & Signature<br>□ PAN □ Aadhaar Saving Bank account no. □ Proof of Identity<br>□ Demat Account ID | | | |

| **Name(s) of holder(s)** | **Signature(s) of holder*** |
|---|---|
| Sole / First Holder (Mr./Ms.) | |
| Second Holder (Mr./Ms.) | |
| Third Holder (Mr./Ms.) | |

*** Signature of witness, along with name and address are required, if the account holder affixes thumb impression, instead of signature**

**# Optional Fields (Information required at Serial nos. 5, 6, 7, 11, 12 & 14 is not mandatory)**

**Note:**

This nomination shall supersede any prior nomination made by the account holder(s), if any.

The Trading Member / Depository Participant shall provide acknowledgement of the nomination form to the account holder(s)

**Name and Signature of Holder(s)***

1._____2._____3_____

* Signature of witness, along with name and address are required, if the account holder affixes thumb impression, instead of signature

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-13

## Declaration Form for opting out of nomination

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| To<br><br>Trading Member/Participant's Name<br><br>Trading Member/Participant's Address | Date | D | D | M | M | Y | Y | Y | Y |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| UCC/DP ID | I | N | | | | | | |
| Client ID (only for Demat account) | | | | | | | | |
| Sole/First Holder Name | | | | | | | | |
| Second Holder Name | | | | | | | | |
| Third Holder Name | | | | | | | | |

I / We hereby confirm that I / We do not wish to appoint any nominee(s) in my / our trading / demat account and understand the issues involved in non-appointment of nominee(s) and further are aware that in case of death of all the account holder(s), my / our legal heirs would need to submit all the requisite documents / information for claiming of assets held in my / our trading / demat account, which may also include documents issued by Court or other such competent authority, based on the value of assets held in the trading / demat account.

**Name and Signature of Holder(s)***

1._____2._____3_____

* Signature of witness, along with name and address are required, if the account holder affixes thumb impression, instead of signature

## Annexure-14

## Demat Debit and Pledge Instruction

| S.No. | Purpose | Signature of Client * |
|---|---|---|
| **1.** | 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 | |
| **2.** | 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. | |
| **3.** | Mutual Fund transactions being executed on Stock Exchange order entry platforms | |
| **4.** | Tendering shares in open offers through Stock Exchange platforms | |

* the same may be signed physically against each purpose of DDPI. The same may also be eSigned. In case of eSign, client shall be given an option for choosing the specific purpose(s) of DDPI.

## Annexure-15

**Format of the Daily Reporting by the members to the Exchange on the amount financed by them under the Margin Trading Facility**

Name of the member
Clearing No.

| Name of Client | Category of Holding (Promoter/Promoter Group or Non Promoter | PAN | Name of Stock or Equity ETF (Collateral or Funded Stock) | Stock Exchange | Quantity Financed (Number of shares or Units of Equity ETFs) | Amount Financed (INR in lakhs) |
|---|---|---|---|---|---|---|
| | | | | | | |

| S. No. | Particulars | (INR in Lakhs) |
|---|---|---|
| 1 | Total outstanding on the beginning of the day | |
| 2 | Add: Fresh exposure taken during the day | |
| 3 | Less: Exposure liquidated during the day | |
| 4 | Net outstanding at the end of the day | |

**Source of Funds**

| | | |
|---|---|---|
| 1 | Out of net worth | |
| 2 | Out of borrowed funds | |
| 3 | If borrowed, name of lenders and amount borrowed to be specified separately | |

**Note:** Disclosure is required to be made on or before 12 noon on the following trading day.

## Annexure-16 : Allocation of collateral

Illustration 1: Consider a self-clearing member (SCM) who has received the following cash collateral from its clients:

| Client | Cash Received (Rs) |
|---|---|
| Client-1 | 2 crore |
| Client-2 | 3 crore |
| Client-3 | 1 crore |
| Client-4 | 1 crore |
| **Total** | **7 crore** |

The member places Rs 6 crore with the CC – Rs 4 crore out of client funds and Rs 2 crore out of proprietary funds. Rs 3 crore worth of client collateral is maintained in the specified client bank account of the member. Few illustrations of allocations and whether permitted or not are provided below:

| Sl. | Allocation | | Comments |
|---|---|---|---|
| 1 | Prop | 2 Cr | Permitted, since total Rs 4 cr is allocated among clients and allocations to individual clients do not exceed the respective collateral provided by them. |
| | Client-1 | 1 Cr | |
| | Client-2 | 1 Cr | |
| | Client-3 | 1 Cr | |
| | Client-4 | 1 Cr | |
| 2 | Prop | 2 Cr | Permitted, since total Rs 4 cr is allocated among clients and allocations to individual clients do not exceed the respective collateral provided by them. |
| | Client-1 | 2 Cr | |
| | Client-2 | 2 Cr | |
| 3 | Prop | 2 Cr | Permitted, since total Rs 4 cr is allocated among clients and allocations to individual clients do not exceed the respective collateral provided by them. |
| | Client-2 | 3 Cr | |
| | Client-3 | 0.5 Cr | |
| | Client-4 | 0.5 Cr | |
| 4 | Prop | 3 Cr | Not permitted, client collateral allocated as proprietary. Total collateral received from clients does not equal amount with the member plus amount allocated. |
| | Client-1 | 2 Cr | |
| | Client-3 | 1 Cr | |
| 5 | Prop | 2 Cr | Not permitted, allocation to Client-3 is in excess from the collateral received from the client. |
| | Client-2 | 2 Cr | |
| | Client-3 | 2 Cr | |
| 6 | Client-1 | 2 Cr | Permitted, proprietary collateral can be allocated as client collateral provided the allocated amount |
| | Client-2 | 3 Cr | |
| | Client-3 | 0.5 Cr | |

| | | | |
|---|---|---|---|
| | Client-4 | 0.5 Cr | does not exceed the actual collateral received from the client. |
| 7 | Client-1 | 4 Cr | Not permitted, although proprietary collateral can be allocated as client collateral, such collateral cannot exceed the actual collateral received from the client |
| | Client-3 | 1 Cr | |
| | Client-4 | 1 Cr | |

Illustration 2:

Suppose a SCM receives the following collateral from clients:

| **Client** | **Collateral Type** | **Value (Rs)** |
|---|---|---|
| Client-1 | Cash | 1 crore |
| Client-2 | Approved securities | 2 crore |
| Client-2 | Non-approved securities | 2 crore |

The member re-pledges the approved securities to the CC. The non-approved securities cannot be provided to the CC. The member provides Rs 1 crore cash collateral of Client1 and Rs 5 crore proprietary cash collateral to the CC. The member may allocate the collateral as follows:

| **Client** | **Value (Rs)** |
|---|---|
| Client-1 | 1 crore |
| Proprietary | 5 crore |

Thus, only the collateral provided to the CC (excluding securities provided through the margin pledge mechanism) shall be allocated. To clarify, Client-2 would still get the benefit of eligible securities collateral re-pledged to CC, however the value for the same shall be assigned by the CC to the account of Client-2, and therefore no collateral allocation shall be done by the member. The non-approved securities collateral would be retained by the member.

If the Client-2 wishes to trade in such a manner that the margin would exceed Rs 2 crore, the member may allocate the proprietary collateral to the client, as follows:

| **Client** | **Value (Rs)** |
|---|---|
| Client-1 | 1 crore |
| Client-2 | 2 crore |
| Proprietary | 3 crore |

## Annexure-17: Treatment of unfunded portion of BG

Consider an example of a SCM with two clients. Suppose the SCM receives the following cash collateral from each of the clients:

| **Client** | **Cash Received (Rs)** |
|---|---|
| Client-1 | 1 crore |
| Client-2 | 1 crore |

Suppose the SCM provides the cash received to a bank and obtains a Bank Guarantee of Rs. 4 crore and provides it to CC. Then, the CM shall allocate the BG as follows:

| **Entity** | **BG Allocation (Rs)** |
|---|---|
| Client-1 | 1 crore |
| Client-2 | 1 crore |
| SCM – Proprietary | 2 crore |

## Annexure-18: Monitoring of the minimum 50% cash-equivalent collateral requirement

Consider the following example of collateral provided by various entities under a CM.

| Entity | Cash-equivalent (A) | Non-cash (B) | Excess cash-eq. If(A>B,A-B,0) | Excess noncash If(B>A,B-A,0) |
|---|---|---|---|---|
| CM Prop | 100 | 40 | 60 | 0 |
| TM-1 Prop | 0 | 0 | 0 | 0 |
| TM-1 Cli-1 | 200 | 250 | 0 | 50 |
| TM-1 Cli-2 | 70 | 10 | 60 | 0 |
| TM-1 Cli-3 | 70 | 100 | 0 | 30 |
| TM-2 Prop | 300 | 200 | 100 | 0 |
| TM-2 Cli-4 | 70 | 90 | 0 | 20 |
| TM-2 Cli-5 | 50 | 100 | 0 | 50 |

Considering TM-1, the excess cash-equivalent collateral of TM-1 Cli-2 cannot be used to offset the excess non-cash collateral of TM-1 Cli-1 and TM-1 Cli-3. Therefore, there will be excess non-cash collateral to the extent of 80 (50 for Cli-1 and 30 for Cli-3) under TM1.

Considering TM-2, the excess proprietary cash-equivalent collateral of TM-2 can be used to offset the excess non-cash collateral of TM-2 Cli-4 and TM-2 Cli-5. Therefore, there will be no excess noncash collateral under TM-2.

Summary of excess cash-equivalent and excess non-cash collateral under CM prop, TM1 and TM-2 would be as under:

| Entity | Excess Cash-eq | Excess noncash |
|---|---|---|
| CM Prop | 60 | - |
| TM-1 | - | 80 |
| TM-2 | 30 | - |

The excess cash-equivalent collateral of TM-2 cannot be used to offset the excess noncash collateral of TM-1. However, the excess cash-equivalent collateral of CM Prop can be used to offset excess non-cash collateral of TM-1. Therefore, the overall excess noncash collateral will be 20, for TM-1.

| Entity | Excess noncash |
|---|---|
| TM-1 | 20 |

The benefit of this excess non-cash collateral (20) will not be available under TM-1. The entities who will get benefit would be identified through a suitable

mechanism by the CCs. In this example, suppose the CC applies FIFO rule and it is assumed that Cli-1 has pledged the non-cash collateral before Cli-3. Therefore, the Cli-1 will receive benefit for its entire collateral (so the effective value of collateral of Cli-1 will be 200+250=450). On the other hand, Cli-3 will not receive benefit of non-cash collateral to the extent of 20 (so the effective value of collateral of Cli-3 will be 70+80 = 150).

## Annexure-19: Blocking of Margins

Suppose the total collateral (allocated collateral plus securities collateral placed through margin pledge/ re-pledge to CC) available against various entities are as given below.

| Entity | Collateral (Rs) |
|---|---|
| CMTM Prop | 1000 |
| TM-1 Prop | 500 |
| TM-1 Cli-1 | 300 |
| TM-1 Cli-2 | 300 |

•Trade-1: TM-1 Cli-2 trades with margin requirement of Rs 100. Blocking of margin shall be as follows:

| Entity | Collateral (Rs) | Blocking (Rs) |
|---|---|---|
| CMTM Prop | 1000 | 0 |
| TM-1 Prop | 500 | 0 |
| TM-1 Cli-1 | 300 | 0 |
| TM-1 Cli-2 | 300 | 100 |

•Trade-2: TM-1 Cli-1 trades with margin requirement of Rs 600. Blocking of margin shall be as follows:

| Entity | Collateral (Rs) | Blocking (Rs) |
|---|---|---|
| CMTM Prop | 1000 | 0 |
| TM-1 Prop | 500 | 300 |
| TM-1 Cli-1 | 300 | 300 |
| TM-1 Cli-2 | 300 | 100 |

•Trade-3: TM-1 Cli-2 trades with revised margin requirement for Cli-2 of Rs 600. Blocking of margin shall be as follows:

| Entity | Collateral (Rs) | Blocking (Rs) |
|---|---|---|
| CMTM Prop | 1000 | 100 |
| TM-1 Prop | 500 | 500 |
| TM-1 Cli-1 | 300 | 300 |
| TM-1 Cli-2 | 300 | 300 |

•Trade-4: TM-1 Cli-2 trades with revised margin requirement for Cli-2 of Rs 900. Blocking of margin shall be as follows:

| Entity | Collateral (Rs) | Blocking (Rs) |
|---|---|---|
| CMTM Prop | 1000 | 400 |
| TM-1 Prop | 500 | 500 |
| TM-1 Cli-1 | 300 | 300 |
| TM-1 Cli-2 | 300 | 300 |

In the above examples, the collateral of Rs 500 blocked from the TM1-Prop, and the collateral of Rs 400 blocked from CMTM Prop, shall be deemed to be allocated to TM-1 Cli-1 and TM-1 Cli-2. The deemed allocation would be as follows:

| Client | Margin (Rs) | Blocked from client collateral (Rs) | Deemed allocation from TM-1 Prop (Rs) | Deemed allocation from CMTM Prop to TM-1 Prop (Rs) |
|---|---|---|---|---|
| TM-1 Cli-1 | 600 | 300 | 300 | 400 |
| TM-1 Cli-2 | 900 | 300 | 600 | |

To clarify, the deemed allocation from CMTM Prop to TM-1 Prop is Rs 400, therefore the total TM-1 Prop collateral (including deemed allocated) would be Rs 900 (Rs 500 + Rs 400). Out of this, the excess client margin would be considered to be deemed allocated to the respective client.

## Annexure-20: Monitoring of risk reduction mode

Suppose the total collateral (allocated collateral plus securities collateral placed through margin pledge/ re-pledge to CC) available against various entities, along with their margin obligations, are as given below.

| CM | TM | Client | Collateral (Rs) | Margin (Rs) | CliMrgn>90% (Rs) |
|---|---|---|---|---|---|
| CM-1 | - | Prop | 1200 | 800 | - |
| CM-1 | TM-1 | Prop | 500 | 400 | - |
| CM-1 | TM-1 | Client-1 | 800 | 780 | 60 |
| CM-1 | TM-1 | Client-2 | 500 | 450 | 0 |
| CM-1 | TM-1 | Client-3 | 400 | 380 | 20 |
| CM-1 | TM-2 | Prop | 500 | 200 | - |
| CM-1 | TM-2 | Client-4 | 1000 | 920 | 20 |
| CM-1 | TM-2 | Client-5 | 1000 | 880 | 0 |

TM level monitoring

In the above table, “CliMrgn>90%”, or client margin in excess of 90%, has been calculated as margin for the client less 90% of the client collateral. Risk reduction mode monitoring for TM shall be based on assessment of [TM Prop Margin + CliMrgn>90%] against the [TM Prop collateral]. Accordingly, margin utilization percentage of TM1 and TM2 would be as under:

• Margin utilization percentage of TM1 = [400 + (60 + 0 + 20)] /500 = 96%

• Margin utilization percentage of TM2 = [200 + (20 + 0)] /500 = 44%

In other words, for TM1, margin of Rs 30 is in excess of 90% of its prop collateral, while there is no excess margin for TM2 against its prop collateral. The same has been tabulated below:

| TM | Total CliMrgn>90% (Rs) | Prop Margin (Rs) | 90% of TM prop collateral (Rs) | TMMrgn>90% (Rs) |
|---|---|---|---|---|
| TM-1 | 80 | 400 | 450 | 30 |
| TM-2 | 20 | 200 | 450 | 0 |

CM level monitoring

In the above table, “TMMrgn>90%”, or TM Margin in excess of 90%, has been calculated as [CliMrgn>90% + TM Prop margin] in excess of 90% of TM prop collateral. Risk reduction mode monitoring for CM shall be based on assessment of [CM Prop Margin + TMMrgn>90%] against the [CM Prop Collateral]. Accordingly, margin utilization percentage of CM1 would be as under:

• Margin utilization percentage of CM1 = [800 + (30 + 0)]/1200 = 69.1%

## Annexure-21: Change of Allocation

Suppose a SCM has following collateral:

| Entity | Cash (Rs) |
|---|---|
| SCM Prop | 200 |
| Cli-1 | 200 |
| Cli-2 | 200 |

Out of the total available cash of Rs 600, suppose the SCM has provided an FDR of Rs 400 to the CC (with Rs 200 cash remaining with the member). Suppose, the FDR provided to the CC is allocated by the SCM as follows. Here, the SCM has chosen not to allocate any collateral to Cli-2 in the total collateral placed with the CC:

| Entity | Collateral allocated (Rs) |
|---|---|
| SCM Prop | 200 |
| Cli-1 | 200 |

Suppose the margin requirement is as follows:

| Entity | Collateral (Rs) | Margin blocked (Rs) |
|---|---|---|
| CM Prop | 200 | 160 |
| Cli-1 | 200 | 150 |

Change in allocation: Example 1

The member shall be permitted to change the allocation as follows (i.e. the member chooses to consider the cash retained with it to be as Rs 50 belonging to Cli-1 and Rs 150 belonging to Cli-2):

| Entity | Collateral (Rs) |
|---|---|
| CM Prop | 200 |
| Cli-1 | 150 |
| Cli-2 | 50 |

Change in allocation: Example 2

The member shall not be permitted to change the allocation as follows (i.e. the member chooses to consider the cash retained with it to be as Rs 100 belonging to each client):

| Entity | Collateral (Rs) |
|---|---|
| CM Prop | 200 |
| Cli-1 | 100 |
| Cli-2 | 100 |

This allocation shall not be permitted since Cli-1 has a margin requirement of Rs 150.

## Annexure-22: Procedures to be followed in Stage-2 and Stage-3

Consider an example of a SCM defaulting in the derivatives segment. An illustration of the cash settlement obligations of prop/clients and attribution of shortage is provided below (the available collateral shown against different entities comprises of both allocated collateral (including deemed allocated) and value of demat securities collateral provided through margin pledge/re-pledge to the level of CC):

| Entity | (Pay-in)/ Pay-out (Rs) | Collateral (Rs) | Position closeout loss (Rs) | Remaining Collateral (Rs) |
|---|---|---|---|---|
| Prop | (3 crore) | 10 crore | 4 crore | 6 crore |
| Client-1 | (3 crore) | 10 crore | 3 crore | 7 crore |
| Client-2 | (3 crore) | 15 crore | 4 crore | 11 crore |
| Client-3 | 2 crore | 15 crore | 2 crore | 13 crore |
| Client-4 | 2 crore | 3 crore | 1 crore | 2 crore |
| **Net Pay-in** | **5 crore** | | | |
| **Shortfall** | **5 crore** | | | |

Scenario 1: All pay-out clients establish not being in default

1.Suppose Client-3 and Client-4 establish within the pre-specified time period that they are not in default, do not have debit balance/dues towards the member and have not received the pay-out due.

2.The remaining collateral of Client-3 and Client-4 (Rs 13 crore and Rs 2 crore respectively), along with the pay-out for the clients (Rs 2 crore each), shall be provided to the clients.

3.The settlement shortfall would now be Rs 9 crore (Rs 5 crore shortfall in net payin, plus Rs 4 crore of pay-out made to Client-3 and Client-4).

4.The settlement shortfall of Rs 9 crore shall be first adjusted with the SCM proprietary pay-in obligation of Rs 3 crore. Excess remaining proprietary collateral of SCM (Rs 3 crore) shall also be used towards the settlement shortfall.

5.Remaining settlement shortfall of Rs 3 crore shall be attributed pro-rata to clients having pay-in, i.e., settlement shortfall of Rs 1.5 crore each shall be attributed to Client-1 and Client-2 and appropriated from their collateral.

Scenario 2: One pay-out client establishes not being in default

1.Suppose Client-3 establishes within the pre-specified time period of not being in

default, not having debit balance/dues towards the member and not having received the pay-out due.

2.The remaining collateral of Client-3 (Rs 13 crore), along with the pay-out (Rs 2 crore), shall be provided to the Client-3.

3.The settlement shortfall would now be Rs 7 crore (Rs 5 crore shortfall in net payin, plus Rs 2 crore of pay-out made to Client-3).

4.The settlement shortfall of Rs 7 crore shall be first adjusted with the SCM proprietary pay-in obligation of Rs 3 crore. Excess remaining proprietary collateral of SCM (Rs 3 crore) shall also be used towards the settlement shortfall.

5.Remaining settlement shortfall of Rs 1 crore shall be attributed pro-rata to clients having pay-in, i.e., settlement shortfall of Rs 0.5 crore each shall be attributed to Client-1 and Client-2 and appropriated from their collateral.

Scenario 3: One pay-out client and one pay-in client establish not being in default

1.Suppose Client-1 and Client-3 establish within the pre-specified time period of not being in default, not having debit balance/dues towards the member and not having received the pay-out due, where applicable.

2.The remaining collateral of Client-1 and Client-3 (Rs 7 crore and Rs 13 crore respectively) shall be provided to them. The pay-out due to Client-3 (Rs 2 crore) shall also be provided to Client-3.

3.The settlement shortfall would now be Rs 7 crore (Rs 5 crore shortfall in net payin, plus Rs 2 crore of pay-out made to Client-3).

4.The settlement shortfall of Rs 7 crore shall be first adjusted with the SCM proprietary pay-in obligation of Rs 3 crore. Excess remaining proprietary collateral of SCM (Rs 3 crore) shall also be used towards the settlement shortfall.

5.Remaining settlement shortfall of Rs 1 crore shall be attributed to Client-2 (since it is established that Client-1 is not in default, no shortage shall be attributed to Client-1).

## Annexure-23: Procedures to be followed in Stage-4

Illustration 1:

Suppose an SCM had no proprietary positions, and the net pay-in obligations were based on five clients. There was a pay-in shortfall of Rs 300, against the net pay-in of Rs 600. Suppose none of the clients could establish within the pre-specified time period of not being in default, not having debit balance/dues towards the member and not having received the pay-out due. Assume there is no position close-out loss. The pay-in shortfall of Rs 300 would be attributed during the Stage 3 on a pro-rata basis from the clients having pay-in obligations. This would be utilized from their available collateral (the available collateral shown against different entities comprises of both allocated collateral (including deemed allocated) and value of securities collateral provided through margin pledge/re-pledge to the level of CC).

| Entity | (PI) / PO (Rs) | Collateral (Rs) | Utilized Collateral (Rs) | Remaining Collateral (Rs) |
|---|---|---|---|---|
| Client-1 | 150 | 200 | 0 | 200 |
| Client-2 | 150 | 100 | 0 | 100 |
| Client-3 | -300 | 300 | 100 | 200 |
| Client-4 | -300 | 300 | 100 | 200 |
| Client-5 | -300 | 300 | 100 | 200 |

Suppose the actual client defaults and position of payables/receivables are identified as follows:

| Entity | Findings | Claim |
|---|---|---|
| Client-1 | Did not receive 150 payout | Pay-out of 150<br>Return of collateral of 200 |
| Client-2 | Did not receive 150 payout | Pay-out of 150<br>Return of collateral of 100 |
| Client-3 | Did not make any pay-in | - |
| Client-4 | Did not make any pay-in | - |
| Client-5 | Had made a pay-in of 300 | Return of collateral of 300 |

Accordingly, the remaining collateral of defaulting clients shall be utilized to fulfil the claims of non-defaulting clients. The additional realization and claim settlement is tabulated below:

| Entity | Additional utilization of collateral | Claim Settled |
|---|---|---|

| | | |
|---|---|---|
| Client-1 | - | Pay-out of 150<br>Return of collateral of 200 |
| Client-2 | - | Pay-out of 150<br>Return of collateral of 100 |
| Client-3 | Additional collateral of 200 utilized | - |
| Client-4 | Additional collateral of 200 utilized | - |
| Client-5 | - | Return of collateral of 100 (from realized) Return of collateral of 200 (from remaining) |

In the event of the remaining collateral of Client-3 and Client-4 not being sufficient (say, due to excess losses in liquidation of positions), the default waterfall of the CC shall be applied for such losses.

Illustration 2:

The following illustration demonstrates the limit on maximum admissible claim against the collateral at the CC by the TM/clients/CP of the defaulting CM. The CC shall recognize the claim of the clients up to the collateral allocated by the CM, plus the value of securities re-pledged till the level of the CC, plus the collateral deemed to be allocated based on the margin requirement of the client. Some examples are tabulated below:

| **Entity** | **Collateral provided to member** | **Margin** | **Collateral allocated by member at CC** | **Value of Securities Re-pledged to CC** | **Collateral deemed allocated (due to margins)** | **Maximum Admissible claim against collateral at CC** |
|---|---|---|---|---|---|---|
| Client-1 | 1000 | 800 | 700 | 300 | 0 | 1000 |
| Client-2 | 1000 | 0 | 400 | 600 | 0 | 1000 |
| Client-3 | 1000 | 0 | 400 | 400 | 0 | 800 |
| Client-4 | 1000 | 800 | 0 | 0 | 800 | 800 |
| Client-5 | 1000 | 0 | 0 | 0 | 0 | 0 |
| Client-6 | 0 | 200 | 100 | 0 | 100 | 0 |

In the last example (Client-6), the CM shall not be permitted to allocate collateral or permit client to trade beyond the available collateral. In case of such violations, the claim shall not be admissible, and the collateral (allocated and/or deemed so) shall be treated as proprietary collateral of the CM.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-24

| Incident Reporting Form | | | |
|---|---|---|---|
| 1. Letter / Report Subject - | | | |
| Name of the Member / Depository Participant -<br>Name of the Stock Exchange / Depository -<br>Member ID / DP ID - | | | |
| 2. Reporting Periodicity<br>Year- | | | |
| ☐ Quarter 1 (Apr-Jun)<br>☐ Quarter 2 (Jul-Sep) | | ☐ Quarter 3 (Oct-Dec)<br>☐ Quarter 4 (Jan-Mar) | |
| 3. Designated Officer (Reporting Officer details) - | | | |
| Name: | Organization : | Title: | |
| Phone / Fax No: | Mobile: | Email: | |
| **Address:** | | | |
| Cyber-attack / breach observed in Quarter:<br>( If yes, please fill **Annexure -24A**)<br>( If no, please submit the NIL report) | | | |
| Date & Time | Brief information on the Cyber-attack / breached observed | | |
| | | | |
| **Annexure -24A** | | | |
| 1. Physical location of affected computer / network and name of ISP - | | | |

| |
|---|
| |

| 2. Date and time incident occurred - | |
|---|---|
| Date: | Time: |

| 3. Information of affected system - | | | | |
|---|---|---|---|---|
| IP Address: | Computer/ Host Name: | Operating System (incl. Ver. / release No.): | Last Patched/ Updated: | Hardware Vendor/ Model: |

| 4. Type of incident - | | |
|---|---|---|
| ☐ Phishing<br>☐ Network scanning /Probing Break-in/Root Compromise<br>☐ Virus/Malicious Code<br>☐ Website Defacement<br>☐ System Misuse | ☐ Spam<br>☐ Bot/Botnet<br>☐ Email Spoofing<br>☐ Denial of Service(DoS)<br>☐ Distributed Denial of Service(DDoS)<br>☐ User Account Compromise | ☐ Website Intrusion<br>☐ Social Engineering<br>☐ Technical Vulnerability<br>☐ IP Spoofing<br>☐ Ransomware<br>☐ Other____ |

| 5. Description of incident - |
|---|
| |

| 6. Unusual behavior/symptoms (Tick the symptoms) - |
|---|

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

7. Details of unusual behavior/symptoms -

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

9. Agencies notified -

| | | | |
|---|---|---|---|
| Law Enforcement | Private Agency | Affected Product Vendor | Other_____ |

10. IP Address of apparent or suspected source -

| Source IP address: | Other information available: |
|---|---|

| 11. How many host(s) are affected - | | |
|---|---|---|
| 1 to 10 | 10 to 100 | More than 100 |

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

## Annexure-25

**Form to report on AI and ML technologies – To be submitted quarterly**

**Intimation to Stock Exchange / Depository for the use of the AI and ML application and systems.**

| SNo. | Head | Value |
|---|---|---|
| 1 | Entity SEBI registration number | |
| 2 | Registered entity category | |
| 3 | Entity name | |
| 4 | Entity PAN no. | |
| 5 | Application / System name | |
| 6 | Date from when the Application / System was used | |
| 7 | Type of area where AI or ML is used | <order execution / Advisory services / KYC / AML / Surveillance / compliance/others (please specify in 256 characters)> |
| 7.a | Does the system involve order initiation, routing and execution? | <Yes / NO> |
| 7.b | Does the system fall under discretionary investment or Portfolio management activities? | <Yes / NO> |
| 7.c | Does the system disseminate investment or trading advice or strategies? | <Yes / NO> |
| 7.d | Is the application/system used in area of Cyber Security to detect attacks | <Yes / NO> |
| 7.e | What claims have been made regarding AI and ML Application / System – if any? | <free text field> |
| 8 | What is the name of the Tool / Technology that is categorized as AI and ML system / Application and submissions are declared vide this response | <free text field> |
| 9 | How was the AI or ML project implemented | <Internally / through solution provider / Jointly with a solution provider or third party> |

| | | |
|---|---|---|
| 10 | Are the key controls and control points in your AI or ML application or systems in accordance to circular of SEBI that mandate cyber security control requirements | <free text field> |
| 11 | Is the AI / ML system included in the system audit, if applicable? | <Yes / NO / NA> |
| 12 | Describe the application / system and how it uses AI / ML as portrayed in the product offering | <free text field> |
| 13 | What safeguards are in place to prevent abnormal behavior of the AI or ML application / System | <free text field> |

## Annexure 26 – Systems deemed to be based on AI and ML technology

Applications and Systems belonging but not limited to following categories or a combination of these:

1. Natural Language Processing (NLP), sentiment analysis or text mining systems that gather intelligence from unstructured data. – In this case, Voice to text, text to intelligence systems in any natural language will be considered in scope. Eg: robo chat bots, big data intelligence gathering systems.

2. Neural Networks or a modified form of it. – In this case, any systems that uses a number of nodes (physical or software simulated nodes) mimicking natural neural networks of any scale, so as to carry out learning from previous firing of the nodes will be considered in scope. Eg: Recurrent Neural networks and Deep learning Neural Networks

3. Machine learning through supervised, unsupervised learning or a combination of both. – In this case, any application or systems that carry out knowledge representation to form a knowledge base of domain, by learning and creating its outputs with real world input data and deciding future outputs based upon the knowledge base. Eg: System based on Decision tree, random forest, K mean, Markov decision process, Gradient boosting Algorithms.

4. A system that uses statistical heuristics method instead of procedural algorithms or the system / application applies clustering or categorization algorithms to categorize data without a predefined set of categories

5. A system that uses a feedback mechanism to improve its parameters and bases it subsequent execution steps on these parameters.

6. A system that does knowledge representation and maintains a knowledge base.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure 27 – Consolidated Quarterly Reporting Form

Consolidated Quarterly report to SEBI of all registered intermediaries with Stock Exchange using AI and ML application and systems for the Quarter Ended DD/MM/YYYY

| Entity registration number | Entity name | Entity PAN no. | Application / System name | Date used from | Type of area where AI or ML is used | To be filled if System Audit is applicable | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | If system audit report is submitted by entity later than "date used from" | | If system audit report is submitted with adverse remarks and Stock Exchange is entitled to inspect the entity | |
| | | | | | | Does system audit report comply to Master Circular dated May 17, 2023 | Is there any adverse comment in the System audit report | Was the entity inspected in pas 1 year | If inspected was any irregularity noted |
| | | | | | <order execution / Advisory services / KYC / AML / Surveillance / compliance/others (please specify in 256 characters)> | <Yes / NO/> | <Yes / NO/> | <Yes / NO> | <Yes / NO> |
| | | | | | | | | | |

## Annexure-28

TLP: AMBER

**CERT-Fin Advisory- 201155100308**

**Advisory for Financial Sector Organisations – RBI and SEBI**

**Overview**

It has been learnt that some of the financial sector institutions are availing or thinking of availing Software as a Service (SaaS) based solution for managing their Governance, Risk & Compliance (GRC) functions so as to improve their cyber security posture. Many a time the risk & compliance data of the institution moves cross border beyond the legal and jurisdictional boundary of India due to the nature of shared cloud SaaS. While SaaS may provide ease of doing business and quick turnaround, it also brings significant risk to the overall health of India's financial sector with respect to data safety and security.

**Description**

If the following data sets fall in the hands of an adversary/cyber attacker, it may lead to unprecedented increase in the attack surface area and weakening of Indian financial sector infrastructure's overall resilience.

- Credit Risk Data
- Liquidity Risk Data
- Market Risk Data
- System & Sub-System Information
- Internal & Partner IP Schema
- Network Topography & Design
- Audit/Internal Audit Data
- System Configuration Data
- System Vulnerability Information
- Risk Exception Information
- Supplier Information & it's dependencies related Data

**Solution**

The Financial Sector organisations may be advised to protect such critical data using layered defence approach and seamless protection against external or insider threat. The organisations may also be advised to ensure complete protection & seamless control over their critical system by continuous monitoring through direct control and supervision protocol mechanisms while keeping such critical data within the legal boundary of India.

The organisations may also be requested to report back to their respective regulatory authority regarding compliance to this advisory.

It is requested that you may kindly keep CERT-In informed of the actions taken and periodically provide the updated compliance to this advisory.

1

(It may be noted that TLP Amber means: Limited disclosure, restricted to participants' organizations.

When should it be used: Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

How may it be shared: Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.)

## Annexure-29

| Root Cause Analysis Form/ RCA | |
|---|---|
| **1. Letter / Report Subject :-** | |
| Name of the stock Broker:<br><br>Exchange Name and Code:<br><br>SEBI Registration number: | |
| **2. Designated Officer and/or Reporting Officer details** | |
| Name: | E-mail:<br><br>Mobile: |
| **3. Date & Time of Incident & Duration of the Incident** | Date:<br><br>Time:<br><br>Duration: |
| | |

| | |
|---|---|
| **4. Incident Description & chronology of events (please use additional sheets if required)** | Brief information on the incident observed |
| **5. Business Impact** | |
| **6. Immediate action taken (please give full details) (Please use additional sheets if required)** | |
| **7. Date & Time of Recovery** | Date:<br><br>Time: |
| **8. Root Cause Summary (Pl attach the detailed Report separately)** | |
| **9. Details of corrective measures taken** | |
| **10. Details of long-term preventive measures taken (please give full details) (please use additional sheets if required)** | |

## Annexure-30

In view of the increasing cybersecurity threat to the securities market, SEBI Regulated Entities (REs) are advised to implement the following practices as recommended by CSIRT-Fin:

1. **Roles and Responsibilities of Chief Information Security Officer (CISO)/ Designated Officer:**
   REs are advised to define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.

2. **Measures against Phishing attacks/ websites:**
   i. The REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. to REs domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.
   ii. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defense. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.
3. **Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):**
   i. All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
   ii. Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time. The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.
4. **Measures for Data Protection and Data breach:**
   i. REs are advised to prepare detailed incident response plan.
   ii. Enforce effective data protection, backup, and recovery measures.
   iii. Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.
   iv. Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.
   v. Deploy data leakage prevention (DLP) solutions / processes.

5. **Log retention:**
   Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. REs are advised to audit that all logsare being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done.
6. **Password Policy/ Authentication Mechanisms:**
   i. Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees Passwords should not be reused across multiple accounts or list of passwords should not be stored on the system.
   ii. Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.
   iii. Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.
7. **Privilege Management:**
   i. Maker-Checker framework should be implemented for modifying the user's right in internal applications.
   ii. For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.
8. **Cybersecurity Controls:**
   i. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
   ii. Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.
   iii. Restrict execution of "powershell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
   iv. Utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
   v. Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.

**9. Security of Cloud Services:**

i. Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.

ii. Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.

iii. Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.

iv. Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.

**10. Implementation of CERT-In/ CSIRT-Fin Advisories:**

The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.

**11. Concentration Risk on Outsourced Agencies:**

i. It has been observed that single third party vendors are providing services to multiple REs, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyber-attack, happens at such organizations, the same could have systemic implication due to high concentration risk.

ii. Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk.

iii. Further, REs also need to take into account this concentration risk while outsourcing multiple critical services to the same vendor.

**12. Audit and ISO Certification:**

i. SEBI's instructions on external audit of REs by independent auditors empaneled by CERT-In should be complied with in letter and spirit.

ii. The REs are also advised to go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE with respect to cybersecurity.

iii. Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits

**Annexure-31**

**Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)**

## 47. Executive Summary

*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction* – NIST Definition.

Cloud computing has common characteristics like on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Due to these characteristics, cloud computing has advantages like reduced IT costs, scalability, business continuity, accessibility anywhere and with any device, higher performance and availability, quick application deployment, 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 framework is based on the study, survey, and consultations done with market participants, regulators, cloud associations, cloud service providers (CSPs), government agencies, and SEBI Advisory Committees. The summary of the framework is as follows:

i. 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.
ii. It is to be noted that 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.

iii. 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:
    1. Utilize the underlying infrastructure of MeitY empaneled CSPs for providing services to the RE.
    2. 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.

iv. 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.

v. 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.

vi. RE shall retain complete ownership of all its data, encryption keys, logs etc. residing in cloud.

vii. Compliance with legal and regulatory requirements, including the requirements provided in this framework, has to be ensured by the RE at all times.

viii. The cloud deployments of RE shall be monitored through Security Operations Centre (SOC) [in-house, third-party SOC or a managed SOC].

ix. 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.

x. The reporting of compliance (with this framework) shall be done by the REs in their systems audit, cybersecurity audit and VAPT reports, and it shall be done in the standardized format notified by SEBI from time to time

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.

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.

Table of Contents

**48. Abbreviations:**

| Sr. No. | Abbreviation | Explanation/Expansion |
|---|---|---|
| 1 | **2FA** | 2 Factor Authentication |
| 2 | **API** | Application Programming Interface |
| 3 | **BCP** | Business Continuity Planning |
| 4 | **CISO** | Chief Information Security Officer |
| 5 | **CSP** | Cloud Service Provider |
| 6 | **DDOS** | Distributed Denial-of-Service |
| 7 | **Dev** | Development Environment |
| 8 | **DR** | Disaster Recovery |
| 9 | **IPS** | Intrusion Prevention System |
| 10 | **LAN** | Local Area Network |
| 11 | **MeitY** | Ministry of Electronics and Information Technology |
| 12 | **MII** | Market Infrastructure Institution |
| 13 | **MPLS** | Multiprotocol Label Switching |

| | | |
|---|---|---|
| 14 | **MSP** | Managed Service Provider |
| 15 | **NIST** | National Institute of Standards and Technology |
| 16 | **P2P** | Point-to-Point connection |
| 17 | **PII** | Personal Identifiable Information |
| 18 | **RE** | Regulated Entity |
| 19 | **SI** | System Integrator |
| 20 | **SLA** | Service Level Agreement |
| 21 | **SOAR** | Security Orchestration, Automation and Response |
| 22 | **SOC** | Security Operations Center |
| 23 | **SSL** | Secure Sockets Layer |
| 24 | **STQC** | Standardization Testing and Quality Certification |
| 25 | **UAT** | User Acceptance Testing |
| 26 | **VAPT** | Vulnerability Assessment & Penetration Testing |
| 27 | **VM** | Virtual Machine |
| 28 | **VPN** | Virtual Private Network |
| 29 | **WAF** | Web Application Firewall |

## 49. Definitions

1. *Cloud Model Description-*

   The description of common cloud deployment models (as per NIST)[105] is given below:

| Sr. No | Model | Description |
|---|---|---|
| **1** | Private Cloud | The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third |

[105] Ref: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

| | | |
|---|---|---|
| | | party, or some combination of them, and it may exist on or off premises. |
| **2** | Community Cloud | The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises |
| **3** | Public Cloud | The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider |
| **4** | Hybrid Cloud | The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. |

2. *Cloud Service Models-*

A. The definitions of various cloud service models (as per NIST)[106] are given below:

i. **Infrastructure as a Service (IaaS)**: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications. The consumer does not directly manage or control the underlying cloud

[106] Ref: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). A few examples of IaaS are Amazon Web Services (AWS) Elastic Compute Cloud, Microsoft Azure, etc.

ii. **Platform as a Service (PaaS)**: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not directly manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. A few examples of PaaS are Google App Engine, Amazon Web Services (AWS) Elastic Beanstalk, etc.

iii. **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. A few examples of SaaS are Gmail, Microsoft Office 365, etc.

B. Other deployment models such as Application as a Service, Security as a Service, etc. may be considered as a sub-part or variant of the above-mentioned models as they contain components of IaaS, PaaS and SaaS. For example, Security as a Service is a form of SaaS which provides specialized information security services. Similarly, Application as a Service is a type of

SaaS in which applications (for example Google sheets, Google docs, etc.) are delivered on-demand to customers through the internet.

3. *Regulated Entity (RE) –*

   The term "Regulated Entity" refers to SEBI registered/ recognized intermediaries (for example brokers, mutual funds, KYC Registration Agencies, and QRTAs) and Market Infrastructure Institutions (Stock Exchanges, Clearing Corporations, and Depositories) regulated by SEBI.

4. *Key Management-*

   In the context of encryption/ decryption, a key is typically a random string of bits generated to hide (encrypt) or reveal (decrypt) data. A key is most commonly used along with an algorithm (method) for encryption/ decryption of data.

   Therefore, Key management refers to management of cryptographic keys in a system, including their (keys') generation, exchange, storage, etc.

5. *Hardware Security Module (HSM)-*

   A Hardware Security Module is a device that is used for management of Keys, as well as for implementing various functions like encryption, decryption, authentication, etc.

*Principle 1: Governance, Risk and Compliance Sub-Framework*

**1. Governance, Risk and Compliance (GRC):**

The REs shall put in place an effective GRC sub-framework for cloud computing to enable them to formulate a cloud strategy suitable for their circumstances/ needs. The RE shall also adhere with the governance framework mentioned in various circulars issued by SEBI. The various aspects that shall be considered by RE (including but not limited to) while formulating the GRC sub-framework are as follows:

i. **Cloud Governance**: The RE shall have a Board/ partners/ proprietors (as the case may be) {hereinafter referred to as "the Board"} approved governance model/ strategy for cloud computing in place. The model/ strategy shall include:
   1. Details of cloud adoption such as cloud service models, deployment models etc.
   2. Type of services to be on boarded on cloud considering various factors such as data classification, criticality of operations, etc. The classification/ categorization shall be done in-line with the circulars/ guidelines issued by SEBI.
   3. Measures to ensure the protection of stakeholder's interests
   4. Measures to comply with the applicable legal and regulatory requirements.

ii. **Cloud Risk Management**:
   1. There is a paradigm shift in the manner of how cloud technology is built and managed in comparison with traditional on–premise infrastructure. Therefore, a comprehensive risk management should be undertaken by the RE to continually identify, monitor, and mitigate the risks posed by cloud computing.
   2. The cloud risk management approach should be approved by the Board of the RE. The cloud risk management approach shall provide details regarding the various risks of cloud adoption such as technical, legal, business, regulatory etc., and the commensurate risk mitigation controls which should be proportionate to the criticality and sensitivity of the data/operations to be on-boarded on the cloud.
   3. As part of risk management process, a thorough risk assessment shall also be done keeping in mind that the RE cannot outsource the risks and decision making associated with deployment of cloud services, to the CSP. The risk assessment shall include (but not limited to) standards like identifying threat sources and events, identifying vulnerabilities and pre-disposing conditions, control analysis, magnitude of impact, etc.

4. A clearly identified and named resource (typically CISO) shall be appointed and shall be responsible for security of the deployments in cloud.

iii. **Compliance and Legal Aspects:** The RE shall have policies, processes, etc. in place to ensure compliance with the applicable legal and regulatory requirements (including but not limited to guidelines, circulars, advisories, etc.) for deployments in cloud, issued by SEBI/ Government of India/ respective state government.

iv. In order to ensure the smooth functioning and adherence with the GRC sub-framework, it is mandated to divide the roles and assign the responsibilities as given below:

1. *Role of the Board/Key Management Personnel (KMP)*- The Board/KMP shall be responsible for:
   a. Approval of cloud governance model and cloud risk management approach, and setting up processes for smooth on boarding on cloud while adhering with all legal, regulatory, technical and business objectives.
   b. Review of cloud governance model and cloud risk management approach as per requirement of the RE. However, the review shall be mandatorily conducted at least once every year.
   c. Setting up the administrative responsibility of senior management.

2. *Role of Senior Management* - The senior management shall be responsible for:
   a. Preparation of and adherence with various policies related to cloud adoption.
   b. Periodic assessment of cloud deployments and mitigation of risks arising out of the same.
   c. Continually monitoring and responding to the risks and intimating the same to board in a timely manner.

d. Assessment, at least on an annual basis, to review the financial and operational condition of the CSP in order to assess its ability to continue to meet the various requirements such as legal, business, compliance, etc. and highlighting any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness to the board in a timely manner.

e. Periodic evaluation of the adherence of the cloud engagement with regulatory, legal and business objectives.

f. Management of Human Resources:

i. Identification of potential skill gaps which emerge as a result of transition to cloud computing.

ii. Capacity building within organization to build adequate skillsets to manage cloud deployments effectively.

3. *Role of IT team*- The IT team shall be responsible for managing day to day operations and assisting senior management in achieving the objectives of cloud deployments.

4. Additional roles/ responsibilities may be added (to the Board/KMP, Senior Management, etc.) as per requirements of the RE.

v. **Grievance Redressal Mechanism**: The RE shall have a robust grievance redressal mechanism, which in no way shall be compromised on account of cloud adoption i.e., responsibility and accountability for redressal of investors'/ members' grievances related to cloud on boarded services shall rest with the RE. Adoption of cloud services shall not affect the rights of the investor/ member against the RE, including the ability of the investor/ member to obtain redressal of grievances as applicable under relevant laws.

vi. **Monitoring and Control of Cloud Deployments**:

1. RE shall have in place a management structure to monitor and control the activities and services deployed on cloud. This shall include, but not limited to, monitoring the performance, uptime (of the systems/ resources) and service availability, adherence to SLA requirements, incident response mechanism, etc.
2. RE shall conduct regular audits/VAPT of its cloud deployments. The frequency and scope of such audits/VAPT shall be in line with SEBI cyber guidelines /circulars /framework issued from time to time.
3. Additionally, the RE shall also assess the performance of the CSP, adequacy of the risk management practices adopted by the CSP, compliance with laws/regulations etc.

vii. **Country Risk**: The engagement with a CSP having country of incorporation/registration outside of India, exposes the RE to country risk. To manage such risk, wherever applicable, the RE shall closely monitor the CSP's country's government policies and its political, social, economic and legal conditions on a continuous basis, and establish sound procedures for mitigating the country risk. This includes, inter alia, having appropriate contingency and exit strategies. In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified.

viii. **Contingency:** The RE shall have appropriate contingency and exit strategies. The RE shall ensure that availability of records to the RE and the supervising authority are not affected under any circumstances, even in case of liquidation of the CSP.

ix. **Miscellaneous**: Any other risk factors deemed relevant/ material by the RE.

*Principle 2: Selection of Cloud Service Providers*

**2. Selection of CSPs:**

The RE shall ensure that the following conditions are met while choosing any Cloud Service Provider (CSP):

i. The storage/ processing of data (DC, DR, near DR etc.) including logs and any other data pertaining to RE in any form in cloud, should be done within the MeitY empaneled CSPs' data centers holding valid STQC (or any other equivalent agency appointed by Government of India) audit status.

ii. For selection of CSPs offering PaaS and SaaS services in India, the RE shall choose only those CSPs which:

1. Utilize the underlying infrastructure/ platform of only MeitY empaneled CSPs for providing services to RE.

2. Host the application/ platform/ services (DC, DR, near DR, etc.) provided to the 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.

3. 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).

iii. Any other additional criteria that the RE considers appropriate/ as per RE's requirement.

iv. The RE shall ensure that storage/ processing/ transfer of its data should be done according to requirements provided in this framework as well as any other regulations/ circulars/ guidelines issued by SEBI and any other Government authorities.

*Principle 3: Data Ownership and Data Localization*

**3. Data Ownership and Localization:**

i. **Data Ownership:** The RE shall retain the complete ownership of all its data and logs, encryption keys, etc. residing in cloud. The CSP shall be working only in a fiduciary capacity. Therefore, the RE, SEBI and any other Government authority authorized under law, shall always have the right to access any or all of the data at any or all point of time.

ii. **Visibility**: Whenever required (by RE/ SEBI), the CSP shall provide visibility to RE as well as SEBI into CSP's infrastructure and processes, and its compliance to applicable policies and regulations issued by SEBI/ Government of India/ respective state government.

iii. **Data Localization**:

In order to ensure that RE and SEBI's right to access RE's data as well as SEBI's rights of search and seizure are not affected by adoption of cloud services, the storage/ processing of data (DC, DR, near DR etc.) including logs and any other data/ information pertaining to RE in any form in cloud shall be done as per the following conditions:

1. The data should reside/be processed within the legal boundaries of India.
2. However, for the investors whose country of incorporation is outside India, the REs shall keep the original data/ transactions/ logs, available and easily accessible in legible and usable form, within the legal boundaries of India.

The RE shall ensure that the above-mentioned requirements are fulfilled at all times during adoption/ usage of cloud services.

iv. It is to be noted that the REs are ultimately responsible and accountable for security of their data (including logs)/ applications/ services hosted in cloud as well as ensuring compliance with laws, rules, regulations, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, RE shall put in place effective mechanism to continuously monitor the CSP and comply with various regulatory, legal and technical requirements notified by SEBI or any other Government authority from time to time.

*Principle 4: Responsibility of the Regulated Entity*

**4. Responsibility of the RE (with respect to CSPs):**

i. While it is acknowledged that there can be a segregation between the RE and the CSP with respect to (including but not limited to) the infrastructure management, and other technical aspects (for example with respect to data, cybersecurity, management of users, etc.), however, the 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 respect to the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.

ii. There shall be an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (including but not limited to technical, managerial, governance related, etc.) of the cloud services between the RE and CSP. 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 shall be a clear delineation and fixing of responsibility for each sub-task/ line-item within the task. The aforementioned delineation of responsibilities shall be added explicitly in the agreement (as an annexure) signed between the RE and the CSP.

iii. In the event of a Managed Service Provider (MSP) or System Integrator (SI) being involved in procurement of cloud services, an explicit and unambiguous delineation/ demarcation of responsibilities shall also be done with respect to MSP/ SI, and the same shall be included in the agreement (in-line with the requirements given above).

iv. Similarly, there shall 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 applicable 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).

v. In view of the fact that a CSP is not a RE, the RE shall continue to have ultimate responsibility and liability for any violation of the laws, rules, regulations, circulars, etc. issued by SEBI or any other authority under any law, regardless of any delineation/ demarcation of responsibilities envisaged in the aforesaid paragraphs.

*Principle 5: Due Diligence by the Regulated Entity*

**5. Due Diligence by the RE (with respect to CSPs):**

i. The REs should evaluate the need, implications (financial, regulatory, etc.), risks, benefits, etc. of adopting cloud computing. The RE shall also conduct its due

diligence with respect to CSPs beforehand and on a periodic basis to ensure that legal, regulatory, business objectives, etc. of the RE are not hampered. The due diligence shall be risk-based depending on the criticality of the data/ services /operations planned to be on boarded on cloud.

ii. A proper due diligence process should be established to assess the capabilities and suitability of a cloud service provider before the engagement.

iii. An analysis (including but not limited to comparative analysis, SWOT analysis, etc.) shall also be conducted on the type of cloud model to be adopted. The analysis should include relevant factors like (including but not limited to) the risks associated with various models, need, suitability, capability of the organization, etc. The above mentioned evaluations / analyses should be conducted keeping in mind that although the IT services/ functionality can be outsourced (to a CSP), REs are ultimately 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 RE's data and logs, and ensuring RE's compliance with respect to the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.

iv. The criteria that an RE shall look out for are (including but not limited to):
    1. Financial soundness of CSP and its ability to service commitments even under adverse conditions.

    2. CSP's capability to identify and segregate RE's data, whenever required.

    3. Security risk assessment of the CSP.

4. Ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to establish data ownership.

5. CSP's ability to effectively service all the RE's customers while maintaining confidentiality, especially where a CSP has exposure to multiple entities.

6. Ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection and confidentiality, SLA, etc.

7. RE shall ensure that CSP performs proper screening and background checks of its personnel and vendors before onboarding, and provides adequate trainings and awareness programs to ensure that the customer (RE) services are not hampered due to misconfiguration/inadvertent actions/operational issues/etc.

8. Capability of the CSP to deal with RE's compliance needs, operational aspects, and ensure information security, data privacy, etc.

9. CSP's ability to ensure compliance with this framework as well as all applicable rules/ regulations/ circulars issued by SEBI from time to time.

10. Any other additional criteria that the RE considers appropriate/ as per RE's requirement.

*Principle 6: Security Controls*

**6. Security Controls[107]:**

The RE shall ensure its compliance with the applicable circulars (for example cybersecurity circular, systems audit circular, DR-BCP circular, etc.)/ guidelines/ advisories, etc. issued by SEBI. Further, in reference to the security controls for adoption of cloud computing[108], the following (including but not limited to) shall be implemented:

6.1. Security of the Cloud:

RE shall perform the assessment of CSPs to ensure that adequate security controls are in place. Some of the common controls (including but not limited to) that the RE needs to check are given below:

i. *Vulnerability Management and Patch Management*:

1. RE shall ensure that CSP has a vulnerability management process in place to mitigate vulnerabilities in all components of the services that the CSP is responsible for (i.e. managed by the CSP). The RE shall assess and ensure that the patch management of CSP adequately covers the components for which the CSP is responsible (i.e. components managed by the CSP). The patch management framework shall include the timely patching of all components coming under the purview of CSP.
2. The RE shall also ensure that CSP conducts Vulnerability Assessment and Penetration Testing (VAPT) for the components managed by the CSP and fixes the issues/ vulnerabilities within the prescribed timelines (as agreed upon by CSP and RE).
3. The RE shall also ensure that the vulnerability management, patch management and VAPT processes are conducted by CSP in-line with the requirements (for example scope, classification of vulnerabilities, duration for closure, etc.) provided in applicable circulars/ guidelines issued by SEBI.

ii. *Monitoring*: RE shall ensure that CSP has adequate security monitoring solutions in place. The monitoring solutions of CSP shall be responsible for the following:

1. Monitoring shall cover all components of the cloud. Additionally, the CSP shall continuously monitor the alerts generated and take appropriate actions as per the defined timelines.
2. The RE shall ensure that any event(s) which may have an impact (financial, reputational, operational, etc.) on the RE shall be intimated to RE by CSP in a timely manner. The reporting should be done in-line with the guidelines/ regulations/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and RE.

iii. *Incident Management*: The RE shall ensure that the CSP has incident management processes in place, to detect, respond and recover from any incident at the earliest. The processes should aim to minimize the impact to the RE.

iv. Wherever Key management is being done by CSP for platform level encryption (for example, full disk encryption or VM level encryption), RE shall assess and ensure that the entire Key lifecycle management is being done by CSP in a secure manner.

v. *Secure User Management*[109]: Wherever the user management is done by CSP, the RE shall ensure that role based access and rule based access are

[107] For CSPs offering PaaS/ SaaS services, in the event any particular security control does not apply to their specific deployment model, such CSPs have to ensure that their vendor/ partner/ sub-contractor providing the underlying infrastructure/ platform fulfils the requirement of the security controls. The RE shall deploy the services of only those PaaS/ SaaS providers which have a back-to-back, clear and enforceable agreement with their vendor/ partner/ sub-contractor for the same.

[108] An indicative mind-map of security controls for cloud deployments is given in Appendix-B

[109] Any type of access/ user provided to SEBI/ any law enforcement agency of Government of India or state government shall be exempt from this clause

strictly followed by CSP for its resources and it shall be based on the principle of least privilege. The following shall also be ensured:

1. Administrators and privileged users shall be given only minimal administrative capabilities for a pre-defined time period, and in response to specific issues/ needs.

2. With respect to administrative privileges/ users, the following shall also be followed:
   a. All administrative privileges/ users shall be tracked via a ticket/ request by the CSP, and the same shall be provided to the RE on request. Further, the RE shall also track any additional privilege granted to any user by the CSP.

   b. Access to systems or interfaces that could provide access to the RE's data is granted only if the RE has given explicit time-limited permission for that access.

3. Multi Factor Authentication shall be used for administrator/ privileged accounts.

4. The necessary auditing and monitoring of the above shall be done by CSP and any anomalies shall be reported to the RE.

vi. *Multi-Tenancy*: In a multi-tenant cloud architecture, the RE shall ensure that CSP has taken adequate controls to ensure that the RE's data (in transit, at rest and in use) shall be isolated and inaccessible to any other tenants. RE shall appropriately assess and ensure the multi tenancy segregation controls placed by CSP and place additional security controls if required. Any access by other tenants/unauthorized access by CSP's resources to RE's data shall be considered as an incident/breach and the CSP shall ensure that the

incident/breach is notified to the RE (as per the norms/ guidelines/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and RE, and adequate steps are taken to control the same. During such incident/breach, the RE shall ensure that CSP should provide all related forensic data, reports and event logs as required to the RE /SEBI /CERT-In/ any government agency for further investigation. All conditions and obligations of the RE and CSP under this framework shall also be applicable in multi-tenancy structure.

vii. The RE shall ensure that the agreement with the CSP contains clause(s) for safe deletion/ erasure of RE's information. The clause should cover various scenarios like business requirement of RE, exit strategy, etc.

viii. For further assurance, the RE may assess the availability of global compliance standards like SOC-2[110] reporting for CSP.

ix. RE shall ensure that CSP has adequate controls (for example anti-virus, encryption of data, micro-segmentation, etc.) in place to safeguard cloud infrastructure as well as to ensure the privacy, confidentiality, availability, processing integrity and security of the RE's data right from data creation/transfer/etc. in the cloud till final expunging of data.

6.2. Security in the Cloud:

RE shall perform risk-based assessment and place adequate controls depending on the criticality of the data/ services/ operations (placed in cloud environment) under the purview of RE. Some of the common controls (including but not limited to) that RE shall put in place are:

6.2.1. Vulnerability Management and Patch Management:

[110] SOC-2 is a voluntary compliance standard for information security developed by American Institute of Certified Public Accountants (AICPA).

The RE shall have a well-defined Vulnerability Management policy in place and should strictly adhere with the same. The policy should also address the vulnerability management aspects of the infrastructure /services /etc. managed by RE in the cloud. The components managed by RE shall be up to date in terms of patches/OS/version etc. The patch management policy shall also mandate timely patch application.

6.2.2. Vulnerability Assessment and Penetration Testing (VAPT):

The VAPT activity undertaken by RE should cover the infrastructure and applications/services hosted by the RE on cloud. The VAPT tactics, tools and procedures should be fine-tuned to test and assess the cloud native risks and vulnerabilities. VAPT should also be conducted before commissioning of any new system. Additionally, the VAPT activity shall be conducted as per the requirements (including scope, classification, duration for closure of vulnerabilities, etc.) provided in applicable circulars/ regulations issued by SEBI.

6.2.3. Incident Management and SOC Integration:

i. The RE shall have incident management policy, procedures and processes in place. The RE shall adhere with the same for deployments being done in cloud.

ii. SOC solution (in-house, third-party SOC or a managed SOC) of RE shall be integrated with the services/ application/ infrastructure deployed by RE in cloud. The continuous monitoring shall be done in an integrated manner and the services/ application/ infrastructure deployed in cloud should be treated as an extension of the RE's on premise network. The SOC shall have complete visibility of information systems of the RE deployed on cloud and should be capable to take SOAR actions across the information systems owned

by the RE. Additionally, only logs, meta-data should be shipped to shared SOC. REs shall ensure that PII/sensitive data should not be shipped to the SOC.

6.2.4. Continuous Monitoring:

Continuous monitoring shall be done by the RE to review the technical, legal and regulatory compliance of CSP and take corrective measures/ ensure CSP takes corrective measures wherever necessary.

6.2.5. Secure User Management:

The RE shall ensure that the following Identity, Authentication and Authorization practices are followed (by CSP as well as by RE):

i. Principle of least privilege shall be adopted for granting access to any resources for normal and admin/privileged accounts.

ii. The identity and access management solution should give the complete view of the access permissions applicable to all resources. The access permissions shall be reviewed regularly in order to remove any unwanted access.

iii. The access logs should be retained and reviewed frequently for any anomalous events.

iv. Time bound access permissions shall be adopted wherever feasible.

v. Multi factor authentication shall be adopted for admin accounts.

6.2.6. Security of Interfaces:

Controls related to typical interfaces in a cloud deployment are given below:

6.2.6.1. Management interface:

i. This is the interface provided to the RE by CSP to manage the infrastructure on cloud. This interface is also used to manage the account of the RE assigned by CSP.

ii. To mitigate the risks, the interface shall have Two Factor Authentication (2FA)/ Multi Factor Authentication (MFA). For additional security, measures such as dedicated lease lines may be explored. The access logs and access list to the interface should be strictly monitored (by RE and CSP). The traffic to and from the interface shall be regulated through firewall, Intrusion prevention system, etc.

6.2.6.2. Internet facing interfaces:

Any interface which is exposed to public at large on the internet in the form of a service/API/etc. is considered as internet facing interface. Adequate security controls such as IPS, Firewall, WAF, Anti DDOS, API gateways etc. should be in place and additional controls such as 2FA authentication, SSL VPN solutions shall also be considered.

6.2.6.3. Interfaces connected between RE's/relevant organizations (Through P2P or LAN/MPLS etc.) and CSP:

Security controls such as IPS, Firewall, WAF, Anti DDOS, etc. shall be in place and additional controls such as IPSEC VPN shall be adopted, wherever necessary, to secure such interfaces.

6.2.7. Secure Software Development:

The RE shall undertake Secure Software Development practices for development of cloud-ready applications which shall include (but not limited to):

i. RE shall adopt appropriate Secure Software Development processes, and security shall be an integral part right from the design phase itself.

ii. A new approach for secure software development shall be implemented by RE for dealing with cloud native development concepts such as micro services, APIs, containers, server less architecture, etc. as the traditional security mechanisms of protecting typical web applications might not be relevant for cloud native development concepts.

iii. Best practices such as zero trust principles, fine grained access control mechanism, API Gateways, etc. shall be adopted for development and usage of APIs. End to end security of the APIs shall also be taken care by the RE as per standard practices and guidelines.

iv. Secure identification, authentication and authorization mechanisms shall be adopted by the RE.

6.2.8. Managed Service Provider (MSP) & System Integrator (SI):

i. Wherever MSP and SI are involved in cloud services procurement, a clear demarcation of roles, and liabilities shall be clearly defined in the Agreement/Contract.

ii. As there are new risks introduced in engaging MSP/SI or both, the same shall be assessed, and mitigated by the RE.

6.2.9. Encryption and Cryptographic Key Management:

i. To ensure the confidentiality, privacy and integrity of the data, encryption as defined below shall be adopted by the RE:

1. Data-at-rest encryption to be done with strong encryption algorithms. Data object encryption, file level encryption or tokenization in addition to the encryption provided at the platform level shall be used.
2. Data-in-motion including the data within the cloud shall be encrypted. Session encryption or data object encryption in addition to the encryption provided at the platform level (Ex. TLS encryption) shall be used wherever any sensitive data is in transit.
3. Data-in-use i.e., wherever data that is being used or processed in the cloud, confidential computing solutions shall be implemented.

ii. To ensure RE's controls on encryption and Key management, the following shall be followed:

1. Wherever applicable:
   a. "Bring Your Own Key" (BYOK) approach shall be adopted, which ensures that the RE retains the control and management of cryptographic keys that would be uploaded to the cloud to perform data encryption.

   b. "Bring Your Own Encryption" (BYOE) approach shall be followed by the RE.

2. In case BYOK and BYOE approaches (as given above) are not implemented by RE, the RE shall conduct a detailed risk assessment and implement appropriate risk mitigation

measures to achieve equivalent functionality/ security to BYOK and BYOE approaches.

3. Generating, storing and managing the keys in a Hardware Security Module (HSM) shall be implemented in a dedicated HSM to have complete control of Key management. However, it is to be noted that HSM should be designed in fault tolerance mode to ensure that the failure of HSM should not have an impact on data retrieval and processing.

6.2.10. End Point Security:

The RE shall ensure that the data security controls in the nature of anti-virus, Data Leak Prevention (DLP) solution etc. are installed and configured on the cloud deployments for effective data security. The RE shall also evaluate the baseline security controls provided by the CSP and may demand additional controls (from CSP) if required.

6.2.11. Network Security:

i. RE shall adopt the micro segmentation principle on cloud infrastructure. Only the essential communication channels between computing resources shall be allowed and the rest of the communication channels shall be blocked.

ii. RE shall also consider the option of utilizing Cloud Access Security Broker (CASB)/ Secure Access Service Edge (SASE)/ similar frameworks or tools for effective monitoring of network, enforcement of policies etc.

6.2.12. Backup and recovery solution:

i. The RE shall ensure that a backup and recovery policy is in place to address the backup requirement of cloud deployments. The backup

and recovery processes shall be checked at least twice in a year to ensure the adequacy of the backups.

ii. The backup shall be logically segregated from production/dev/UAT environment to ensure that the malware infection in such systems does not percolate to backup environment.

iii. Wherever CSP's backup services are utilized, adequate care should be taken with encryption solution and Key management.

6.2.13. Skillset:

RE shall equip staff overseeing cloud operations with the knowledge and skills required to securely use and manage the risks associated with cloud computing. The skills should also be imparted to oversee the management interfaces, security configurations etc. of CSP infrastructure. This is a critical factor as it will reduce the misconfigurations, vulnerabilities etc. and will increase the reliability of services.

6.2.14. Breach Notification:

CSP shall notify the RE of any cybersecurity incident (for example data breach, ransomware, etc.) as mandated by the RE. The reporting shall be done as per the norms/ guidelines/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and RE. The CSP shall provide all related forensic data, reports and event logs as required by RE/ SEBI/ CERT-In/ any other government agency. The incident shall be dealt as per the Security Incident Management Policy of the RE along with the relevant guidelines/ directions issued by SEBI/ Government of India/ respective state government.

*Principle 7: Contractual and Regulatory Obligations*

**7. Contractual and Regulatory Obligations[111]:**

i. A clear and enforceable cloud service provider engagement agreement should be in place to protect RE's interests, risk management needs, and ability to comply with supervisory expectations.

ii. 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.

iii. The contract/agreement shall be vetted with respect to legal and technical standpoint by the RE. The agreement shall be flexible enough to allow the RE to retain adequate control over the resources which are on boarded on cloud. The agreement should also provide RE the right to intervene with appropriate measures to meet legal and regulatory obligations.

iv. SEBI/ CERT-In/ any other government agency shall at any time:

1. 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.
2. 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.

3. Engage a forensic auditor to identify the root cause of any incident (cyber security or other incidents) related to RE.
4. Seek the audit reports of the audits conducted by CSP.

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.

v. The RE shall also ensure that adequate provisions are included in the agreement/ contract for the following audit/ VAPT functions-
   1. CSP shall be responsible for conducting audit/ VAPT of the services/ components managed by the CSP.
   2. The RE shall be responsible for conducting audit/ VAPT of the services/ components managed by the RE. The audit/ VAPT shall be conducted as per the requirements (including scope, duration for closure of vulnerabilities, etc.) provided in various applicable circulars/ regulations issued by SEBI from time to time.
   3. Implementation and configuration audit of the resources to be deployed by the RE in cloud environment shall be conducted by the RE and the same shall be certified by the RE after closing all non-compliances/ observations before go-live.
   4. The RE may take into consideration the report/certificate of the audit of the CSP conducted by STQC. However, wherever required, CSP has to conduct additional audits (from CERT-In empaneled auditors) to fulfil all the requirements provided in various applicable circulars/ regulations issued by SEBI, and the same shall be ensured by the RE.

[111] With respect to CSPs offering PaaS/SaaS services, REs shall deploy the services of only those CSPs which have a back-to-back, clear and enforceable agreement with their vendor/ partner/ sub-contractor providing their underlying infrastructure/ platform for fulfilling the requirements provided in this Principle.

5. The RE shall ensure that appropriate clauses/ terms (including SLA clauses) are added in the agreement (signed between RE and CSP) to enforce the above-mentioned audit/ VAPT requirements.

vi. Contract/Agreement should have adequate provisions regarding the termination of contract with CSP, and appropriate exit strategies to ensure smooth exit without hindering any legal, regulatory or technical obligations of the RE.

vii. As part of exit strategy, a clear expunging clause shall be defined in agreement with CSP, which shall state that whenever the RE intends to expunge the data, CSP shall securely and permanently erase the RE's data in disks, backup devices, logs, etc. and no data shall remain in recoverable form. However, it is the responsibility of the RE to ensure that the minimum retention requirements for data (including logs) as prescribed by SEBI/ Government of India/ respective state government are met and that the required data, logs, etc. are archived, even if the RE moves out of the cloud/ changes CSPs.

viii. The RE shall ensure that their data (including but not limited to logs, business data, etc.) is stored in an easily accessible, legible and usable manner (during utilization of cloud services and after exit from the cloud) and it shall be provided to SEBI/ any other government agency whenever required.

ix. The RE is required to adhere with SEBI circulars/ guidelines issued from time to time and the cloud framework shall be seen as an addition/ complementary to existing circulars/ guidelines and not as a replacement.

x. The agreement/contract made by RE shall also include (but not limited to) below mentioned terms/ provisions/ clauses:

1. Definition of the IT activities and resources being on boarded on cloud, including appropriate service and performance standards including for the material sub-contractors, if any.

2. Effective access to all the objects/ information relevant to the RE/ RE's operation including data, books, records, logs, alerts, and data centre.
3. Continuous monitoring and assessment of the CSP by the RE so that any necessary corrective measure can be taken immediately, including termination of contract and any minimum period required to execute such provisions, if deemed necessary.
4. Type of material adverse events (e.g., data breaches, denial of service, service unavailability etc.) and incident reporting requirements to the RE to take prompt mitigation and recovery measures and ensure compliance with statutory and regulatory guidelines.
5. Compliance with the provisions of IT Act, other applicable legal requirements and standards to protect the customer (RE) data.
6. The deliverables, including SLAs, for formalizing the performance criteria to measure the quality and quantity of service levels.
7. Storage of data (as applicable to the RE) within the legal boundaries of India as per extant regulatory requirements.
8. Clauses requiring the CSP to provide details of data (captured, processed and stored) related to RE and RE's customers to SEBI/ any other government agency.
9. Controls for maintaining confidentiality of data of RE and its customers, and incorporating CSP's liability to the RE in the event of security breach and leakage of such information.
10. Types of data/ information that the CSP is permitted to share with the RE's customers and/or any other party.
11. Specifying the resolution process for events of default, insolvency, etc. and indemnities, remedies, and recourse available to the respective parties.
12. Contingency plan(s) to ensure business continuity planning, RPO/RTO, and recovery requirements.

13. Provisions to fulfill the search and seizure requirements (as provided above in this principle) and audit/ VAPT requirements (as provided above in this principle).
14. Right to seek information (by RE/ SEBI) from the CSP about the third parties (in the supply chain) engaged by the CSP.
15. Clauses making the CSP contractually liable for the performance and risk management practices of its sub-contractors.
16. Obligation of the CSP to comply with directions issued by SEBI in relation to the activities of the RE on boarded on cloud.
17. Termination rights of the RE, including the ability to orderly transfer the proposed cloud onboarding assignment to another CSP, if necessary or desirable.
18. Obligation of the CSP to co-operate with the relevant authorities in cases involving the RE as and when required.
19. Clauses for performing risk assessment by CSP with respect to hiring of third party vendors, the checks/ process followed by CSP before onboarding personnel/ vendors, etc.
20. Any other provision(s) required to ensure compliance with respect to circulars/ guidelines/ regulations (including this cloud framework) issued by SEBI.

xi. Wherever the System integrator or managed service provider or both, along with CSP are involved, the contractual terms and agreement shall unambiguously demarcate/ delineate the roles, and liabilities of each participating party (in-line with the "*Principle 4: Responsibility of the RE"* of the framework) for each task/ activity/ function. There shall be no "joint/ shared ownership" for any task/ activity/ function/ component.

xii. If any function/ task/ activity has to be performed jointly by the RE and CSP/MSP/SI, there shall 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 aforementioned delineation of responsibilities shall be added explicitly in the agreement (as an annexure) signed between the RE and the CSP (and MSP/SI wherever applicable). However, any such clause in the agreement shall not absolve the RE from having the ultimate responsibility and liability for any violation of the laws, rules, regulations, circulars, etc. issued by SEBI or any other authority under any law, regardless of any delineation/ demarcation of responsibilities.

xiii. Similarly, there shall 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 applicable 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.

xiv. **Reporting Requirements**:

1. It is being reiterated that the 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 applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government.
2. The RE shall explicitly and unambiguously specify the party (RE or CSP/MSP/SI) which is responsible for ensuring compliance with each clause

of the applicable SEBI circulars (for example cybersecurity circular, systems audit, etc.) in its audit reports. There shall be no "joint/ shared ownership" for any of the clauses. In case the responsibility of ensuring compliance (for any clause) rests with both parties, the task shall be split into sub-tasks/line-items, and for each sub-task/line-items, the responsible party shall be indicated in the report.

3. The RE shall ensure that the demarcation/ delineation of responsibilities is provided for each clause of the applicable SEBI circular(s).
4. In view of the above requirements, as well as to ensure effective monitoring of cloud deployments by REs, reporting of compliance (with this framework) shall be done by the REs in their systems audit, cybersecurity audit and VAPT reports, and it shall be done in the standardized format notified by SEBI from time to time.
5. **Reporting by Auditor**: 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 (including the tasks/ functions stated in clause (x) above, wherever applicable).
   b. For each clause of applicable/ relevant SEBI circular/ guidelines/ regulations.

   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).

xv. In the event of any CSP deployed by an RE losing its empanelment status with MeitY/ commits a passive breach of contract/ agreement in any way, the RE shall ensure that it becomes compliant with this framework within 6 (six) months of being notified of/ discovering the breach.

*Principle 8: BCP, Disaster Recovery & Cyber Resilience*

**8. Business Continuity Planning (BCP), Disaster Recovery & Cyber Resilience:**

i. The RE shall assess its BCP framework and ensure that it is in compliance with this cloud framework as well as other guidelines/ circulars issued by SEBI from time to time.

ii. RE shall also assess the capabilities, preparedness and readiness with respect to cyber resilience of CSP. The same can be periodically assessed by conducting DR drills (in accordance with circulars/ guidelines issued by SEBI) by involving necessary stakeholders.

iii. Additionally, RE shall develop a viable and effective contingency plan to cope with situations involving a disruption/ shutdown of cloud services.

*Principle 9: Vendor Lock-In and Concentration Risk Management*

**9. Concentration Risk Management:**

i. RE shall assess its exposure to CSP lock-in and concentration risks. The risk evaluation shall be done before entering into contract/ agreement with CSP and the same should also be assessed on a periodic basis.

ii. In order to mitigate the CSP concentration risks, RE shall explore the option of cloud-ready and CSP agnostic solutions (such as implementing multi-cloud ready solutions) which can facilitate the RE in migrating the solutions as and when necessary, with minimal changes. Exit strategies shall be developed, which should consider the pertinent risk indicators, exit triggers, exit scenarios, possible migration options, etc.

iii. The RE shall also take measures to implement data portability and inter-operability as part of exit/ transfer strategy.

iv. In order to mitigate the risk arising due to failure/ shutdown of a particular CSP, and to limit the impact of any such failure/ shutdown on the securities market, SEBI may specify concentration limits on CSPs (thereby setting a limit on the number of REs that a CSP may provide its services to).

**10. Recommendations:**

i. 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.

ii. REs are solely accountable for all aspects related to the cloud services adopted by them including but not limited to availability of cloud applications, confidentiality, integrity and security of their data and logs, and ensuring RE's compliance with respect to the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.

iii. While deploying cloud services, the REs shall adopt the nine (9) principles as provided in this framework:

1. Principle 1: Governance, Risk and Compliance Sub-Framework
2. Principle 2: Selection of Cloud Service Providers
3. Principle 3: Data Ownership and Data Localization
4. Principle 4: Responsibility of the Regulated Entity
5. Principle 5: Due Diligence by the Regulated Entity
6. Principle 6: Security Controls
7. Principle 7: Contractual and Regulatory Obligations
8. Principle 8: BCP, Disaster Recovery & Cyber Resilience
9. 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.

iv. The cloud services shall be taken only from the 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:
    1. Utilize the underlying infrastructure/ platform of only MeitY empaneled CSPs for providing services to the RE.
    2. Host the application/ platform/ services provided to RE, and 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.
    3. 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).

v. 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).

vi. Similarly, 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).

vii. 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

   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.

viii. 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.

ix. SEBI/ CERT-In/ any other government agency shall at any time:
    1. 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.
    2. 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.
    3. Engage a forensic auditor to identify the root cause of any incident (cyber security or other incidents) related to RE.
    4. Seek the audit reports of the audits conducted by CSP.

    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.

x. 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.

xi. Transition Period:
    1. For the REs which are not utilizing any cloud services currently, the framework shall be applicable/ come into force from the date of issuance.
    2. For the REs which are currently utilizing cloud services, upto 12 months shall be given to ensure their compliance with the framework. Additionally, such REs shall provide regular milestone-based updates as follows:

| SN. | Timeline | Milestone |
|---|---|---|
| 1 | Within one (1) month of issuance of framework | REs shall provide details of the cloud services, if any, currently deployed by them. |
| 2 | Within three (3) months of issuance of framework | The REs shall submit a roadmap (including details of major activities, timelines, etc.) for the implementation of the framework |
| 3 | From three (3) to twelve (12) months of issuance of framework | Quarterly progress report as per the roadmap submitted by the RE. |
| 4 | After twelve (12) months of issuance of framework | Compliance with respect to the framework to be reported regularly |

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

xii. 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.

***Appendix-A***

**Format for Submission of Details of Cloud Deployments**

The REs shall provide details of their cloud deployment in the following format-

*A. Entity Name:*

*B. Entity Type: (For example stock exchange, depository, mutual fund, etc.)*

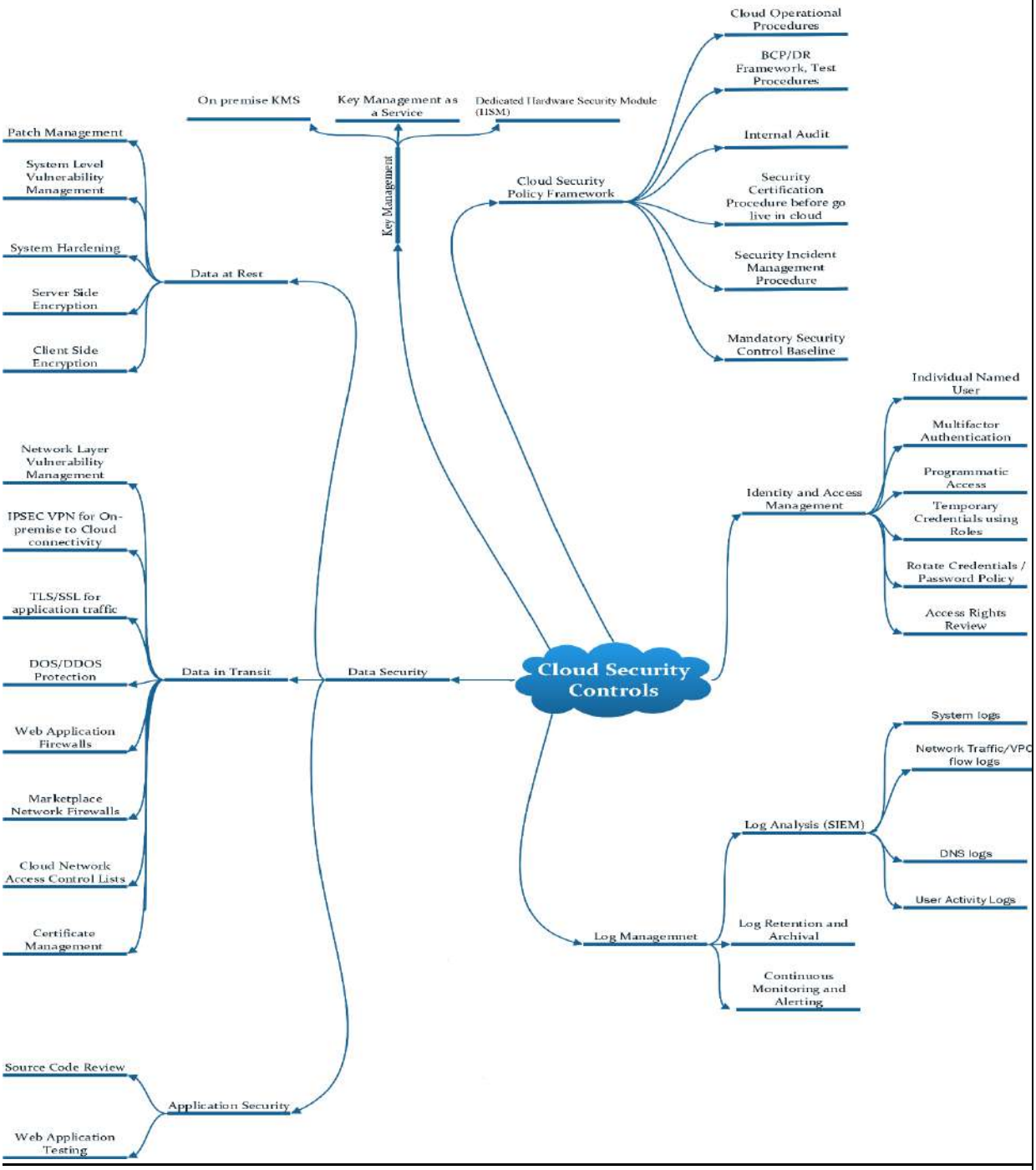
*C. Whether Utilizing Cloud Services? Yes/ No*

*For Each Cloud application/ service/ system, please provide a response to the following:*

| SN | Details Required | ***Entity Response*** |
|---|---|---|
| 1 | Name of the Application/ Service/ System | |
| 2 | The type of deployment model utilized (public cloud, community cloud, etc.) | |
| 3 | The type of service model utilized (For example IaaS, PaaS, etc.) | |
| 4 | Name of the Cloud Service Provider (CSP) | |
| 5 | Country of incorporation/ registration of CSP | |
| | Name of the Managed Service Provider (MSP) / System Integrator (SI) [wherever applicable] | |
| 6 | Country of incorporation/ registration of MSP/ SI | |
| 7 | Whether the application/ service/ system is a critical or core application/ service/ system? | |
| 8 | Details of Data hosted/ stored in cloud | |
| 9 | Whether data is stored within the legal boundaries of India? | |

***Appendix-B***

## Indicative Mindmap for Cloud Security



भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-32

**Format for reporting changes in "status or constitution" of Members**

Name of the Stock Exchange:
Report for the quarter ending: June/September/December/March Year:-
Date of report:

| S. No. | Date of receipt | Name of the member | Registration number INB/F/EINS | Type of change | Details of changes | | PAN (incoming entities) | Date of Change | Date of approval by Stock Exchange |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | **Pre** | **Post** | | | |
| | | | | | | | | | |
| | | | | | | | | | |

| **Type** | Description of Change |
|---|---|
| **I** | Amalgamation, demerger, consolidation or any other kind of corporate restructuring falling within the scope of section 230 of the Companies Act, 2013 or the corresponding provision of any other law for the time being in force. |
| **II** | Change in managing director, whole-time director or director appointed in compliance with clause (v) of sub-rule (4A) of rule 8 of the Securities Contracts (Regulation) Rules, 1957. |
| **III** | Change in control. |
| **IV** | Any change between the following legal forms - individual, partnership firm, Hindu undivided family, private company, public company, unlimited company or statutory corporation and other similar changes. |
| **V** | In case of a partnership firm any change in partners not amounting to dissolution of the firm. |
| **VI** | Any other purpose as may be considered appropriate by the Stock Exchanges. |

**Guidelines to fill up the format and sending the same to SEBI**

1. A separate annexure shall be submitted for each "Type of change" as specified in the format.
2. The report shall be signed by an authorized representative of the Stock Exchange and the same shall be stamped.
3. The Stock Exchanges shall furnish the report to SEBI by 7th day of month following the end of each quarter.
4. The report shall be submitted by e-mail at serpa@sebi.gov.in. A hard copy of the report shall also be submitted to SEBI.

## Annexure-33

**Declaration-Cum-Undertaking**

We M/s. (*Name of the intermediary/the acquirer/person who shall have the control*), hereby declare and undertake the following with respect to the application for prior approval for change in control of (*name of the intermediary along with the SEBI registration no.*):

1. The applicant/intermediary (Name) and its principal officer, the directors or managing partners, the compliance officer and the key management persons and the promoters or persons holding controlling interest or persons exercising control over the applicant, directly or indirectly (*in case of an unlisted applicant or intermediary, any person holding twenty percent or more voting rights, irrespective of whether they hold controlling interest or exercise control, shall be required to fulfill the 'fit and proper person' criteria*) are fit and proper person in terms of Schedule II of SEBI (Intermediaries) Regulations, 2008.
2. We bear integrity, honesty, ethical behaviour, reputation, fairness and character.
3. We do not incur following disqualifications mentioned in Clause 3(b) of Schedule II of SEBI (Intermediaries) Regulations, 2008 i.e.
    i. No criminal complaint or information under section 154 of the Code of Criminal Procedure, 1973 (2 of 1974) has been filed against us by the Board and which is pending.
    ii. No charge sheet has been filed against us by any enforcement agency in matters concerning economic offences and is pending.
    iii. No order of restraint, prohibition or debarment has been passed against us by the Board or any other regulatory authority or enforcement agency in any matter concerning securities laws or financial markets and such order is in force.
    iv. No recovery proceedings have been initiated by the Board against us and are pending.
    v. No order of conviction has been passed against us by a court for any offence involving moral turpitude.
    vi. No winding up proceedings have been initiated or an order for winding up has been passed against us.
    vii. We have not been declared insolvent.
    viii. We have not been found to be of unsound mind by a court of competent jurisdiction and no such finding is in force.
    ix. We have not been categorized as a wilful defaulter.
    x. We have not been declared a fugitive economic offender.
4. We have not been declared as not 'fit and proper person' by an order of the Board.
5. No notice to show cause has been issued for proceedings under SEBI(Intermediaries) Regulations, 2008 or under section 11(4) or section

11B of the SEBI Act during last one year against us.

6. It is hereby declared that we and each of our promoters, directors, principal officer, compliance officer and key managerial persons are not associated with vanishing companies.
7. We hereby undertake that there will not be any change in the Board of Directors of incumbent, till the time prior approval is granted.
8. We hereby undertake that pursuant to grant of prior approval by SEBI, the incumbent shall inform all the existing investors/ clients about the proposed change prior to effecting the same, in order to enable them to take informed decision regarding their continuance or otherwise with the new management.

The said information is true to our knowledge.

(stamped and signed by the Authorised Signatories)

**Annexure-34**

**APPLICATION TO SEBI FOR OPENING OF WHOLLY OWNED SUBSIDIARIES, STEP DOWN SUBSIDIARIES OR ENTERING INTO JOINT VENTURES IN GIFT IFSC**

**Please read the instructions carefully before filling up the Application form:**

1. **Fill in all the particulars clearly.**
2. **The information should be complete in all respects.**
3. **Please attach the relevant enclosures.**
4. **The application shall be submitted through Stock Exchange / Clearing Corporation along with NOC obtained from all the Stock Exchanges/ Clearing Corporations/Depositories, where the applicant is a member/participant and other documents as listed in the present form.**

---

II. **GENERAL INFORMATION:**

| | | |
|---|---|---|
| 1 | Details of all registrations of the applicant company in India and abroad | 1. Name of the entity (Earlier name, if any)<br>2. Type of Intermediary (If Broker, names of Exchanges and if DP, name of the Depositories)<br>3. Registration Number<br>4. Date of Registration |
| 2 | Networth of the applicant company (in Rs.) | |
| 3 | Details of the following persons:<br>a) Promoters (Name and PAN number)<br>b) Directors ( Name, DIN and PAN number)<br>c) Key Person of the applicant (Name and PAN number) | |
| 4 | Details of regulatory action taken/ initiated/ pending, if any, against the applicant/ promoters/ directors/key personnel/ principal officer of the applicant company (in India/abroad) | |

| | | |
|---|---|---|
| 5 | Any fee remaining unpaid to SEBI by applicant/ associates | |
| 6 | Amount of proposed investment (converted in Indian Rupees) | |
| 7 | Whether the applicant is setting up a Wholly Owned subsidiary (WOS) or a Step Down Subsidiary (SDS) or entering into Joint Venture (JV) or acquiring stake in an existing company. | |
| 8 | Details of the proposed WOS/SDS/JV in GIFT IFSC (provide relevant details in case of equity participation in existing company or joint venture with a company) | a) Name of the proposed entity in GIFT IFSC<br>b) Purpose for setting up the WOS/SDS/JV/Equity Participation etc.<br>c) Nature of proposed activities |

2. **UNDERTAKING**

a) Pursuant to setting up Wholly Owned Subsidiary / investment in step down subsidiary/joint venture, etc., we shall maintain networth for each category of registration as per SEBI Act, 1992 & Regulations/ circulars issued there under and bye laws/ rules/ regulations/ circulars, etc. issued by respective stock exchanges/Depositories.

**Signature**

**Name**

**Designation**

**Place:**
**Date:**

**III. ENCLOSURES:**

a. Certificate of Networth:
   i) Networth Certificate of the applicant based on the latest audited results (in Rs.), duly certified by a Chartered Accountant.

ii) In case the above Networth Certificate is more than 6 months old, then provide i) above as well as the latest provisional networth certificate, duly certified by a Chartered Accountant.

b. NOC obtained from all the Stock Exchanges/Depositories where the applicant is a member/ participant, in case the applicant is a Stock Broker/Depository Participant.

c. Details of any non-compliance w.r.t 'fit and proper person' criteria as specified in Schedule II of SEBI (Intermediaries) Regulations, 2008.

d. Declaration cum undertaking (format enclosed) with regard to compliance with the 'fit and proper person' criteria as specified in Schedule II of SEBI (Intermediaries) Regulations, 2008 duly stamped and signed by the Authorized Signatories of the applicant.

e. Latest shareholding pattern of the applicant and list of the shareholders who have controlling interest.

**Declaration Cum Undertaking**

We M/s. Name of the intermediary, having SEBI registration certificate in the capacity of _____ bearing registration number _____ hereby declare and undertake the following w.r.t our application for setting up WOS/SDS/JV in GIFT IFSC:

1. Name of the intermediary and its principal officer, directors or managing partners, compliance officer, key management persons, promoters or persons holding controlling interest or persons exercising control over the intermediary directly or indirectly and person holding twenty percent or more voting rights of the intermediary (hereinafter referred to as "We" or "Us") are fit and proper person as per requirement laid down in Schedule II of SEBI (Intermediaries) Regulations, 2008.

2. We bear integrity, honesty, ethical behaviour, reputation, fairness and character.

3. We do not incur following disqualifications mentioned in Clause 3(b) of Schedule II of SEBI (Intermediaries) Regulations, 2008 i.e.

   (i) No criminal complaint or information under section 154 of the Code of Criminal Procedure, 1973 (2 of 1974) has been filed against us by the Board and which is pending.

(ii) No charge sheet has been filed against us by any enforcement agency in matters concerning economic offences and is pending.

(iii) No order of restraint, prohibition or debarment has been passed against us by the Board or any other regulatory authority or enforcement agency in any matter concerning securities laws or financial markets and such order is in force.

(iv) No recovery proceedings have been initiated by the Board against us and are pending.

(v) No order of conviction has been passed against us by a court for any offence involving moral turpitude.

(vi) No winding up proceedings have been initiated or an order for winding up has been passed against us.

(vii) We have not been declared insolvent.

(viii) We have not been found to be of unsound mind by a court of competent jurisdiction and no such finding is in force.

(ix) We have not been categorized as a wilful defaulter.

(x) We have not been declared a fugitive economic offender.

4. We have not been declared as not 'fit and proper person' by an order of the Board.
5. No notice to show cause has been issued for proceedings under SEBI (Intermediaries) Regulations, 2008 or under section 11(4) or section 11B of the SEBI Act during last one year against us.
6. It is hereby declared that we and each of our Promoters, Directors, Principal Officer, Compliance Officer and Key Managerial Persons are not associated with vanishing companies.
7. There is no outstanding SEBI fee payable by the intermediary.

The said information is true to our knowledge.

(stamped and signed by the Authorised Signatories)

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-35 - Information regarding Grievance Redressal Mechanism

Dear Investor,

In case of any grievance / complaint against the Stock Broker / Depository Participant:

Please contact Compliance Officer of the Stock Broker/ Depository Participant (Name) / email-id (xxx.@email.com) and Phone No. - 91-XXXXXXXXXX.

You may also approach CEO/ Partner/Proprietor (Name) / email-id (xxx.@email.com) and Phone No. - 91-XXXXXXXXXX.

If not satisfied with the response of the Stock Broker/ Depository Participant, you may contact the concerned Stock Exchange / Depository at the following:

| | Web Address | Contact No. | Email-id |
|---|---|---|---|
| NSE | www.bseindia.com | xxxxxxxxxx | xxx@bseindia.com |
| BSE | www.nesindia.com | Xxxxxxxxxx | xxx@nse.co.in |
| MSEI | www.msei.in | xxxxxxxxxx | xxx@msei.in |

| | Web Address | Contact No. | Email-id |
|---|---|---|---|
| CDSL | www.cdslindia.com | xxxxxxxxxx | xxx@cdslindia.com |
| NSDL | www.nsdl.co.in | xxxxxxxxxx | xxx@nsdl.co.in |

You can also lodge your grievances with SEBI at http://scores.gov.in. For any queries, feedback or assistance, please contact SEBI Office on Toll Free Helpline at 1800 22 7575 / 1800 266 7575.

## Annexure-36

Investor Charter – Stock Brokers

**VISION**

To follow highest standards of ethics and compliances while facilitating the trading by clients in securities in a fair and transparent manner, so as to contribute in creation of wealth for investors.

**MISSION**

i) To provide high quality and dependable service through innovation, capacity enhancement and use of technology.

ii) To establish and maintain a relationship of trust and ethics with the investors.

iii) To observe highest standard of compliances and transparency.

iv) To always keep 'protection of investors' interest' as goal while providing service.

**Services provided to Investors**

- Execution of trades on behalf of investors.
- Issuance of Contract Notes.
- Issuance of intimations regarding margin due payments.
- Facilitate execution of early pay-in obligation instructions.
- Settlement of client's funds.
- Intimation of securities held in Client Unpaid Securities Account (CUSA) Account.
- Issuance of retention statement of funds.
- Risk management systems to mitigate operational and market risk.
- Facilitate client profile changes in the system as instructed by the client.
- Information sharing with the client w.r.t. exchange circulars.
- Redressal of Investor's grievances.

**Rights of Investors**

- Ask for and receive information from a firm about the work history and background of the person handling your account, as well as information about the firm itself.
- Receive complete information about the risks, obligations, and costs of any investment before investing.
- Receive recommendations consistent with your financial needs and investment objectives.
- Receive a copy of all completed account forms and agreements.
- Receive account statements that are accurate and understandable.
- Understand the terms and conditions of transactions you undertake.
- Access your funds in a timely manner and receive information about any restrictions or limitations on access.
- Receive complete information about maintenance or service charges, transaction or redemption fees, and penalties.
- Discuss your grievances with compliance officer of the firm and receive prompt attention to and fair consideration of your concerns.

**Various activities of Stock Brokers with timelines**

| S.No. | Activities | Expected Timelines |
|---|---|---|
| 1. | KYC entered into KRA System and CKYCR | 10 days of account opening |
| 2. | Client Onboarding | Immediate, but not later than one week |
| 3. | Order execution | Immediate on receipt of order, but not later than the same day |
| 4. | Allocation of Unique Client Code | Before trading |
| 5. | Copy of duly completed Client Registration Documents to clients | 7 days from the date of upload of Unique Client Code to the Exchange by the trading member |
| 6. | Issuance of contract notes | 24 hours of execution of trades |
| 7. | Collection of upfront margin from client | Before initiation of trade |
| 8. | Issuance of intimations regarding other margin due payments | At the end of the T day |

| | | |
|---|---|---|
| 9. | Settlement of client funds | Monthly/ Quarterly for running account settlement (RAS) as per the preference of client.<br>If consent not given for RAS – within 24 hours of pay-out |
| 10. | 'Statement of Accounts' for Funds, Securities and Commodities | Weekly basis (Within four trading days of following week) |
| 11. | Issuance of retention statement of funds/commodities | 5 days from the date of settlement |
| 12. | Issuance of Annual Global Statement | 30 days from the end of the financial year |
| 13. | Investor grievances redressal | 30 days from the receipt of the complaint |

## DOs and DON'Ts for Investors

| DOs | DON'Ts |
|---|---|
| 1. Read all documents and conditions being agreed before signing the account opening form.<br>2. Receive a copy of KYC, copy of account opening documents and Unique Client Code.<br>3. Read the product / operational framework / timelines related to various Trading and Clearing & Settlement processes. | 1. Do not deal with unregistered stock broker.<br>2. Do not forget to strike off blanks in your account opening and KYC.<br>3. Do not submit an incomplete account opening and KYC form. |
| 4. Receive all information about brokerage, fees and other charges levied.<br>5. Register your mobile number and email ID in your trading, demat and bank accounts to get regular alerts on your transactions.<br>6. If executed, receive a copy of Power of Attorney. However, Power of Attorney is not a mandatory requirement as per SEBI / Stock Exchanges. Before granting Power of Attorney, carefully examine the scope and implications of powers being granted.<br>7. Receive contract notes for trades executed, showing transaction price, brokerage, GST and STT etc. as | 4. Do not forget to inform any change in information linked to trading account and obtain confirmation of updation in the system.<br>5. Do not transfer funds, for the purposes of trading to anyone other than a stock broker. No payment should be made in name of employee of stock broker.<br>6. Do not ignore any emails / SMSs received with regards to trades done, from the Stock Exchange and raise a |

| | |
|---|---|
| applicable, separately, within 24 hours of execution of trades.<br>8. Receive funds and securities / commodities on time within 24 hours from pay-out.<br>9. Verify details of trades, contract notes and statement of account and approach relevant authority for any discrepancies. Verify trade details on the Exchange websites from the trade verification facility provided by the Exchanges.<br>10. Receive statement of accounts periodically. If opted for running account settlement, account has to be settled by the stock broker as per the option given by the client (30 or 90 days).<br>11. In case of any grievances, approach stock broker or Stock Exchange or SEBI for getting the same resolved within prescribed timelines. | concern, if discrepancy is observed.<br>7. Do not opt for digital contracts, if not familiar with computers.<br>8. Do not share trading password.<br>9. Do not fall prey to fixed / guaranteed returns schemes.<br>10. Do not fall prey to fraudsters sending emails and SMSs luring to trade in stocks / securities promising huge profits.<br>11. Do not follow herd mentality for investments. Seek expert and professional advice for your investments. |

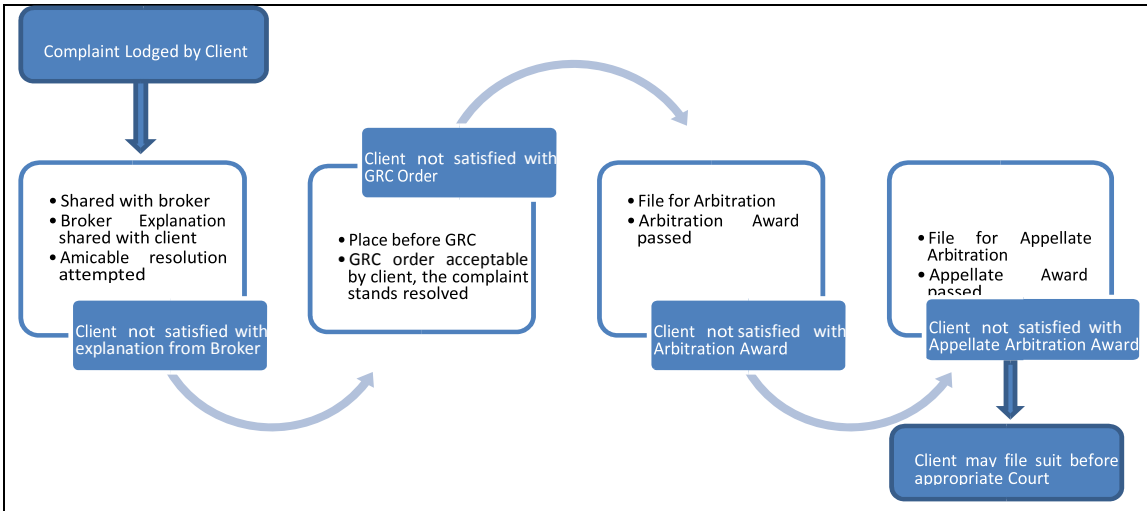
Grievance Redressal Mechanism

**Level 1 –** Approach the Stock Broker at the designated Investor Grievance e-mail ID of the stock broker. The Stock Broker will strive to redress the grievance immediately, but not later than 30 days of the receipt of the grievance.

**Level 2 –** Approach the Stock Exchange using the grievance mechanism mentioned at the website of the respective exchange.

**Level 3 –** The complaint not redressed at Stock Broker / Stock Exchange level, may be lodged with SEBI on SCORES (a web based centralized grievance redressal system of SEBI) @ https://scores.gov.in/scores/Welcome.html

Complaints Resolution Process at Stock Exchange explained graphically:




**Timelines for complaint resolution process at Stock Exchanges against stock brokers**

| S. No. | Type of Activity | Timelines for activity |
|---|---|---|
| 1. | Receipt of Complaint | Day of complaint (C Day). |
| 2. | Additional information sought from the investor, if any, and provisionally forwarded to stock broker. | C + 7 Working days. |
| 3. | Registration of the complaint and forwarding to the stock broker. | C+8 Working Days i.e. T day. |
| 4. | Amicable Resolution. | T+15 Working Days. |
| 5. | Refer to Grievance Redressal Committee (GRC), in case of no amicable resolution. | T+16 Working Days. |
| 6. | Complete resolution process post GRC. | T + 30 Working Days. |
| 7. | In case where the GRC Member requires additional information, GRC order shall be completed within. | T + 45 Working Days. |
| 8. | Implementation of GRC Order. | On receipt of GRC Order, if the order is in favour of the investor, debit the funds of the stock broker. Order for debit is issued immediately or |

| | | |
|---|---|---|
| | | as per the directions given in GRC order. |
| 9. | In case the stock broker is aggrieved by the GRC order, will provide intention to avail arbitration | Within 7 days from receipt of order |
| 10. | If intention from stock broker is received and the GRC order amount is upto Rs.20 lakhs | Investor is eligible for interim relief from Investor Protection Fund (IPF). The interim relief will be 50% of the GRC order amount or Rs.2 lakhs whichever is less. The same shall be provided after obtaining an Undertaking from the investor. |
| 11. | Stock Broker shall file for arbitration | Within *3 months*[112] from the date of GRC recommendation |
| 12. | In case the stock broker does not file for arbitration within *3 months*[5] | The GRC order amount shall be released to the investor after adjusting the amount released as interim relief, if any. |

**Handling of Investor's claims / complaints in case of default of a Trading Member / Clearing Member (TM/CM)**

**Default of TM/CM**

Following steps are carried out by Stock Exchange for benefit of investor, in case stock broker defaults:

•Circular is issued to inform about declaration of Stock Broker as Defaulter.

•Information of defaulter stock broker is disseminated on Stock Exchange website.

•Public Notice is issued informing declaration of a stock broker as defaulter and inviting claims within specified period.

[112] Words *"6 months"* replaced with *"3 months"* in view of Circular - SEBI/HO/MIRSD/DOS3/P/CIR/dated June 3, 2022.

•Intimation to clients of defaulter stock brokers via emails and SMS for facilitating lodging of claims within the specified period.

Following information is available on Stock Exchange website for information of investors:

•Norms for eligibility of claims for compensation from IPF.

•Claim form for lodging claim against defaulter stock broker.

•FAQ on processing of investors' claims against Defaulter stock broker.

•Provision to check online status of client's claim.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-37

**Format for Investor Complaints Data to be displayed by Stock Brokers on their respective websites**

**Data for every month ending**

| SN | Received from | Carried forward from previous month | Received during the month | Total Pending | Resolved* | Pending at the end of the month** | | Average Resolution time^ (in days) |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Pending for less than 3 months | Pending for more than 3 months | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | 8 |
| 1 | Directly from Investors | | | | | | | |
| 2 | SEBI (SCORES) | | | | | | | |
| 3 | Stock Exchanges | | | | | | | |
| 4 | Other Sources (if any) | | | | | | | |
| 5 | Grand Total | | | | | | | |

**Trend of monthly disposal of complaints**

| SN | Month | Carried forward from previous month | Received | Resolved* | Pending** |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | April -YYYY | | | | |
| 2 | May-YYYY | | | | |
| 3 | June-YYYY | | | | |
| 4 | July-YYYY | | | | |
| | …. | | | | |
| | ….. | | | | |
| | March-YYYY | | | | |
| | Grand Total | | | | |

*Should include complaints of previous months resolved in the current month, if any.

**Should include total complaints pending as on the last day of the month, if any.

^Average resolution time is the sum total of time taken to resolve each complaint in the current month divided by total number of complaints resolved in the current month.

**Trend of annual disposal of complaints**

| SN | Year | Carried forward from previous year | Received during the year | Resolved during the year | Pending at the end of the year |
|---|---|---|---|---|---|
| 1 | 2017-18 | | | | |
| 2 | 2018-19 | | | | |
| 3 | 2019-20 | | | | |
| 4 | 2020-21 | | | | |
| 5 | 2021-22 | | | | |
| | **Grand Total** | | | | |

## Annexure-38

**To be on Stamp / Franked Paper of appropriate value and notarized**

**AFFIDAVIT OF UNDERTAKING CUM INDEMNITY BOND TO BE SUBMITTED BY MEMBER TO ……. [NAME OF THE STOCK EXCHANGE / CLEARING CORPORATION]**

**This Undertaking cum Indemnity Bond is signed at Mumbai on this _____day of _____, 20.**

**By**

I/We, Member of …….. **[Name of The Stock Exchange / Clearing Corporation]** (bearing Trading / Clearing No. _____), having office at ……, (hereinafter referred to as "**Member**", which expression, unless repugnant to the context or meaning thereof, shall be deemed to include its successors and assigns).

In favour of:

……..Ltd., **[Name of the Stock Exchange / Clearing Corporation]** a company incorporated under the Companies Act, 1956 having its registered office at …… (hereinafter referred to as "…..", which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and assigns).

I/We hereby solemnly declare and undertake that:

Whereas the Securities and Exchange Board of India (hereinafter referred to as **"SEBI**") has issued circular dated July 01, 2020 on Standard Operating Procedure to be followed in the case of trading member/clearing member leading to default (hereinafter referred to as the "said circular").

Whereas in terms of the said circular the …….. [Name of the Stock Exchange / Clearing Corporation] has amended its bye-laws and is empowered …….. [Name of the Stock Exchange / Clearing Corporation] to issue instructions to the concerned bank/s to freeze the bank account/s maintained by the Member, for all debits / withdrawal by the Member in the event of a potential default by the Member in meeting its obligations to Stock Exchange / Clearing Member / Clearing Corporation and / or repayment of funds / securities to his / its clients.

**Now, in consideration of the above, I / We do hereby agree and confirm unconditionally to undertake that:**

1) …… [Name of the Stock Exchange / Clearing Corporation] is empowered to instruct the concerned banks to freeze my / our bank accounts for all debits / withdrawals from such accounts. The details of bank accounts held by me/ us are as follows:

2) Any debits to such bank account, post freezing by the banks, shall be done only on the express instructions to the said banks by …… [Name of the Stock Exchange/ Clearing Corporation].

3) …… [Name of the Stock Exchange / Clearing Corporation] shall not be liable in any way to me/us for any losses, claims, penalties, proceedings / actions, damages, consequential or otherwise, arising there from or occasioned thereby.

4) No proceeding/suit/action/claims would be adopted by me/us against …… [Name of the Stock Exchange/ Clearing Corporation] for any act done with respect to issuance of instruction to the bank/s mentioned above for freezing of my/our account/s held with the bank/s.

5) I / We agree to indemnify and keep …… [Name of the Stock Exchange/ Clearing Corporation] and/or its successors/assigns indemnified from time to time, and at all times hereafter, against all claims, demands, damages, liabilities, proceedings, losses, actions, charges and expenses made or suffered or incurred or caused or likely to suffer / incur directly or indirectly, to …… [Name of the Stock Exchange/ Clearing Corporation] and/or its successors/assigns on account of freezing of my/our account/s held with bank/s.

6) I/ We shall keep the Bank appropriately notified of the obligations undertaken by me / us herein and authorizing them to honour the instructions from …… [Name of the Stock Exchange / Clearing Corporation].

7) I / We undertake that a revised Undertaking cum Indemnity Bond shall be submitted by me / us to …… [Name of the Stock Exchange / Clearing Corporation] within seven working days of opening of any new bank account or change in details of any existing bank account,

8) This Undertaking cum Indemnity Bond shall be binding on my / our successors, legal representatives and assigns.

9) I / We warrant that representations made by the undersigned / on behalf of the Member are true and correct.

IN WITNESS WHEREOF, I/We hereby execute this Undertaking cum Indemnity Bond on the day, month and year above written.

Solemnly declared at )
this ___ day of _____, 20 ) BEFORE ME

(Name of Designated Director)
(Name of Trading Member)
(with rubber stamp & SEBI Registration No.) In the presence of:

1.

2.

Note: Board Resolution for execution of the said undertaking cum indemnity and authorization for signing the same should be enclosed along with the document**.**

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

## Annexure-39 – Digital Mode of Payment

| Date | Department of SEBI | Name of Intermediary / Other entities | Type of Intermediary | SEBI Registration No. (If any) | PAN | Amount (Rs) | Purpose of Payment (including the period for which payment was made e.g. quarterly, annually) | Bank name and Account number from which payment is remitted | UTR No. |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |

## Annexure-40

Following FMC circulars shall stand repealed and relevant SEBI circulars shall be applicable to all commodity derivatives exchanges including regional commodity derivative exchanges for compliance by their members.

| S. No. | Subject | FMC Circular being repealed | SEBI circulars being made applicable |
|---|---|---|---|
| I | Segregation of Client and Own Funds and Securities | No circular issued by FMC | a) SMD/SED/CIR/93/23321 dated Nov 18, 1993.<br>b) MRD/DoP/SE/Cir-11/2008 dated Apr 17, 2008. |
| Ii | Running Account Settlement | a) FMC/4/2012/C/14 No. 1/2/2012/IR-I/Client-Protect/ dated Feb 02, 2012.<br>b) FMC/4/2013/C/59 No. 1/2/2012/IR-I/Client-Protect dated May 20, 2013.<br>c) No. 1/2/2012/IR-I/Client-Protect dated Jun 25, 2013.<br>d) FMC/4/2014/C/121 FMC/2014/04/23-Quarterly Settlement dated Oct 17, 2014. | a) Clause 12 of Annexure A to MIRSD/ SE /Cir-19/2009 dated Dec 3, 2009.<br>b) MIRSD /Cir/ 01/ 2011 dated May 13, 2011. |
| Iii | Requirements with respect to Financial Documents, PAN, Inactive Clients etc. | a) No.IRD/Div/(1)FMCR/1/2005 dated Feb 14, 2006.<br>b) Div. III/I/(53)/06/PAN No. dated Nov 28, 2006.<br>c) 9/3/2008-MKT-II dated Jan 12, 2009.<br>d) No. 18/1/2007/MKT-III dated Feb 11, 2008.<br>e) No. 9/1/2009-MKT-I dated Dec 07, 2009.<br>f) No. 9/12009-MKT-I dated | a) Clauses 6,8,14,15,16,18 and 19 of Annexure A to MIRSD/ SE /Cir-19/2009 dated Dec 03, 2009.[113]<br>b) CIR/MIRSD/01 /2013 dated Jan 04, 2013.<br>c) CIR/MIRSD/64/2016 dated Jul 12, 2016.<br>For new client accounts. |

[113] Words "*Clauses 1 to 11 and Clauses 14 to 19 of Annexure A to MIRSD /SE/Cir-19/2009 dated Dec 3, 2009*" replaced with "*Clause 6,8,14,15,16,18 and 19 of Annexure A to MIRSD/SE/CIR-19/2009 dated December 03, 2009*" in view of Clauses 1,2,3,4,5,7,9,10,11 and 17 of SEBI Circular dated December 03, 2009, being incorporated in various provisions of SEBI Circular CIR/MIRSD/16/2011 dated August 22, 2011 and FMC Circular FMC/4/2011/G/30 dated December 16, 2011 and Annexures specified in these circulars.

| | | | |
|---|---|---|---|
| | | Aug 10, 2010. | |
| Iv | In-Person Verification | Part C of FMC/4/2015/C/0015No. FMC/COMPL/IV/KRA-05/11/14 dated Mar 13, 2015. | a) Para 3 of MIRSD/Cir- 26 /2011 Dec 23, 2011.<br>b) Point 4 of Part 'Instructions/Check List' of Annexure 3 of Circular CIR/MIRSD/16/2011 dated Aug 22, 2011. |
| V | KRA | FMC/4/2015/C/0015 No. FMC/COMPL/IV/KRA-05/11/14 dated Mar 13, 2015 | a) MIRSD/Cir-23/2011 dated Dec 2, 2011.<br>b) Para 1 of MIRSD/Cir- 26 /2011 dated Dec 23, 2011. |
| Vi | Anti-Money Laundering and Maintenance of Records | a) No.7/1/2008- MKT-II dated Oct 30, 2009.<br>b) No.7/1/2008-MKT-II dated Jan 25, 2010.<br>c) No. 7/1/2008-MKT-II dated Aug 25, 2010.<br>d) FMC/4/2013/C/163; Div. III / I/ 89 / 07 dated Dec 18, 2013.<br>e) No. 7/1/2013-MKT-1(A) dated Feb 04, 2015. | a) CIR/ISD/AML/3/2010 dated Dec 31, 2010.<br>b) CIR/MIRSD/2/2013 dated Jan 24, 2013.<br>c) CIR/MIRSD/1/2014 dated Mar 12, 2014. |
| Vii | Dealing in Cash | FMC/2/2014/C/23 No. 9/1/2014 -MKT-I dated Mar 12, 2014. | MRD/SE/Cir- 33/2003/27/08 dated Aug 27, 2003. |
| viii | Guidelines on Pre-funded Instruments | FMC/4/2011/G/0010FMC/Compl t/Circular dated Sep 27, 2011. | CIR/MIRSD/03/2011 dated Jun 9, 2011. |
| Ix | SMS and Email alerts facility to clients | a) FMC/4/2012/C/13 No. FMC/IR-I/Client protection/2012 dated Feb 02, 2012.<br>b) FMC/Complt/Circular dated Jun 04, 2012.<br>c) No:IR (2)/5/2012/SMS-Email dated Dec 07,2012.<br>d) No.IR(2)/5/2012/SMS-Email dated Jan 21, 2013.<br>e) No.IR(2)/5/2012/SMS/Email dated Mar 01, 2013.<br>f) No.IR(2)/5/2012/SMS/Email dated Mar 06, 2013.<br>g) No.IR(2)/5/2012/SMS/Email dated May 15, 2013. | CIR/MIRSD/15/2011 dated Aug 02, 2011. |

| | | | |
|---|---|---|---|
| | | h) No.IR(2)/5/2012/SMS/E-mail dated Jun 21, 2013. | |
| X | Contract Note | a) No. 07/2008/COMP/LAD-ENF/AD(SN)/6609 dated Oct 27, 2009.<br>b) FMC/COMPL/IV/2010/03/05/00011 dated Apr 19, 2011.<br>c) Div.III/I/89/07 dated Mar 13, 2014.<br>d) Div.III/I/89/07 dated Dec 24, 2014. | a) SMDRP/Policy/Cir-56/2000 dated Dec 15, 2000.<br>b) SMD/SE/15/2003/29/04 dated Apr 29, 2003.<br>c) MRD/DoP/SE/Cir-20/2005 dated Sep 8, 2005.<br>d) Clause 13 of Annexure A to MIRSD/ SE /Cir-19/2009 dated Dec 3, 2009. |
| Xi | Exclusive e-mail ID for redressel of Investor Complaints | No circular issued by FMC | MRD/DoP/Dep/SE/Cir-22/06 dated Dec 18, 2006. |
| Xii | Display of information such as logo, registration number on notice board and contract note and investor grievance redressal mechanism on notice board | No circular issued by FMC | a) Cir/MIRSD/ 9 /2010 dated Nov 4, 2010.<br>b) CIR/MIRSD/3/2014 dated Aug 28, 2014. |
| Xiii | Internal Audit | No circular issued by FMC | Para 7 to 11 of circular MIRSD/Master Cir-04/2010 dated Mar 17, 2010. |
| Xiv | Inspection of brokers | a) No. Div./III/I/301/2011-12/Audit dated Dec 23, 2011.<br>b) No. Div./III/I/104/2008-09/Audit dated Feb 02, 2012.<br>c) FMC/1/2014/C/50No.Div.III/I/300/2011-12/Audit dated Apr 23, 2014.<br>d) FMC/1/2014/C/47 No. FMC/1/2014/Audit/C Dated Apr 23, 2014. | a) Para 2 to 6 of circular MIRSD/Master Cir-04/2010 dated Mar 17, 2010.<br>b) CIR/MIRSD/13/2012 dated Dec 07, 2012. |
| xv | Change in control/ constitution | a) No.IRD-Div-III/1/143/10-MR dated Aug 14, 2010.<br>b) Div:III/I/120/MR-2011/2 dated Apr 07, 2011.<br>c) FMC/6/2011/C/0018 No. | a) MIRSD/MSS/Cir- 30/ 13289/03 dated Jul 09, 2003.<br>b) CIR/MIRSD/2/2011 dated Jun 3, 2011. |

| | | | |
|---|---|---|---|
| | | Div.III/I/68/MR/General dated Sep 22, 2011.<br>d) FMC/6/2011/C/0019 No. Div. III/I/157/10-MRDated Sep 27, 2011.<br>e) FMC/4/2012/C/41 No. Div. III/I/157/10-MR dated Apr 04, 2012.<br>f) Div. III/I/10/MR dated Apr 30, 2015. | c) CIR/MIRSD/14/2011 dated Aug 02, 2011. |
| Xvi | Procedure for surrender of membership | a) FMC/6/2011/C/0018 No. Div.III/I/68/MR/General dated Sep 22, 2011.<br>b) FMC/1/2014/C/146 dated Dec 31, 2014.<br>c) No.Div.II/I/112/2015/Refund of Deposit dated Jan 19, 2015.<br>d) No. III/I/10/MR dated Jul 08, 2015. | MIRSD/MSS/Cir- 30/ 13289/03 dated Jul 09, 2003. |
| Xvii | Guidelines on Outsourcing of Activities by Intermediaries | No circular issued by FMC | CIR/MIRSD/24/2011 dated Dec 15, 2011. |
| xviii | BPO/KPO services - Segregation thereof from Commodity Derivatives Market | No. S/1/2009/MD-I dated Mar 28, 2011. | a) Rule 8(1)(f) and 8(3)(f) of SCRR, 1957.<br>b) SMD/POLICY/CIR-6//97 dated May 07, 1997. |
| xix | Authorized Persons | No.6/3/2008-MKT – II; FMC/2/2012/G/3 dated Jan 11, 2012. | a) MIRSD/ DR-1/ Cir- 16 /09 dated Nov 06, 2009.<br>b) Cir/MIRSD/AP/8/2010 dated Jul 23, 2010. |

## Annexure-41

Following FMC circulars are specific to commodity derivatives market. Contents/norms specified in following circulars shall continue to be in force beyond September 28, 2016. Provisions of these circulars shall be applicable to all commodity derivatives exchanges including regional commodity derivatives exchanges for compliance by their members.

| S. No. | Subject | FMC Circular No. and Date |
|---|---|---|
| I | Account Opening Process | a) No.-FMC/4/2011/G/30 Ref. No.: Div. III/I/89/07 dated Dec 16, 2011*.<br>b) Div.III/I/89/07 dated Aug 23, 2013.<br>c) F.No.FMC/COMPL/2013/10/30-FSLRC/FSDC dated Mar 28, 2014.<br>d) Div.III/2/89/VOL IV dated Apr 23, 2014.<br>e) No. FMC/COMPL/IV/KRA-05/11/14 dated Feb 26, 2015. |
| Ii | Customer Protection such as keeping evidence of client placing order | No.FMC/Comp/VI/2009/04/06/114/5787 dated Sep 16, 2009. |
| Iii | Nomenclature of Stock brokers | a) 4/5/2005- M&S/MCX/Unit-II dated Apr 25, 2006.<br>b) No.IRD-DIV-III/I/FCR-I/2009 dated Dec 21, 2009.<br>c) No. DIV-III/I/122/10/MR dated Jun 25, 2010.<br>d) 6/3/2008-MKT – II dated Feb 18, 2011. |
| Iv | Surrender of membership | F.No.1/4/2009/MD-I dated Jul 20, 2009. |

*All clauses to remain except to the extent as modified as described below. Annexure - 3 (Rights and Obligations of Members, Authorized Persons and Clients) of Circular No.-FMC/4/2011/G/30 Ref. No.: Div. III/I/89/07 dated Dec 16, 2011 is modified as follows:

In Clause 30, for the words "in the Statement immediately but not later than 30 calendar days of receipt thereof, to the Member. A detailed statement of accounts must be sent every month to all the clients in physical form. The proof of delivery of the same should be preserved by the Member" the words "in the Statement within such time as may be prescribed by the relevant Exchange from time to time where the trade was executed, from the receipt thereof to the Stock broker" shall be substituted.

In Clause 31, for the words "monthly" the words "daily" shall be substituted.

Para 3 C.A.iv which restricted seeking authorization through non-mandatory documents for any adjustment of funds among securities (stock) exchange and commodities exchange, will not be applicable, if such adjustment is within the same broking entity.

## Annexure-42

Following FMC circulars shall stand repealed.

| S. No. | Subject | FMC Circular No. and Date |
|---|---|---|
| i | Segregation of Client Accounts in Commodity Futures Exchange and Spot Exchanges | FMC/2/2011/C/0008; No.9/1/2011-MKT/I dated Sep 26, 2011. |
| ii | Member to obtain FMC Unique Code | No. IRD/Div./III/(1)/FMCR/1/2005 dated Oct 28, 2005. |
| iii | Submission of networth certificate from the members | No. Div-III/I/122/10/MR dated Nov 22, 2010. |
| iv | Nomenclature of Stock Brokers | No. IRD-DIV-III/I/FCR-I/2009 dated Dec 21, 2009. |
| | | No. DIV-III/I/122/10/MR dated Jun 25, 2010. |
| | | 6/3/2008-MKT –II dated Feb 18, 2011. |

## APPENDIX - LIST OF CIRCULARS / COMMUNICATION

| Sr. no | Circular/ Notification No. and Date | Subject |
|---|---|---|
| 1. | SEBI communication SE/10118 dated October 12, 1992. | Listing fees from 1992-93 to 1996-97. |
| 2. | SMD/SED/CIR/93/23321 dated November 18, 1993. | Regulation Of Transactions Between Clients and Brokers. |
| 3. | SMD/VRN/1476/95 dated April 27, 1995. | Severance of connections with other businesses. |
| 4. | SMD/POLICY/CIR-6/97 dated May 07, 1997. | Applicability of Rule 8(1)(f) and 8(3)(f) of the Securities Contract (Regulation) Rules, 1957. |
| 5. | SMD/POLICY/CIRCULAR/30/97 dated November 25, 1997 | Registration of Brokers. |
| 6. | SMD/POLICY/CIR-34/97 dated December 11, 1997. | Conversion of individual membership into Corporate membership. |
| 7. | SMD/POLICY/CIR-11/98 dated March 16, 1998. | Additional information to be submitted at the time of registration of Stock Broker with SEBI. |
| 8. | FITTC/DC/CR-1/98 dated June 16, 1998. | Derivatives Trading in India. |
| 9. | SMD/POLICY(BRK.REG.)/CIR-18/98 dated July 09, 1998. | Merger/ Amalgamation of Trading Members. |
| 10. | SMDRP/POLICY/CIR- 06/2000 dated January 31, 2000. | Conditions to be met by Broker for providing Internet Based Trading Service. |
| 11. | SMDRP/Policy/Cir-48/2000 dated October 11, 2000. | Securities Trading through Wireless medium on Wireless Application Protocol (WAP) platform. |
| 12. | SMDRP/POLICY/CIR-56/00 dated December 15, 2000 | Use of Digital Signature on Contract Notes |
| 13. | SMDRP/POLICY/CIR-39/2001 dated July 18, 2001. | Unique Client Code. |
| 14. | SMD/POLICY/CIR-49/2001 dated October 22, 2001. | Advertisement by Brokers/ Sub-Brokers and grant of trading terminals. |
| 15. | SMD/DBA-II/CIR-22/2002 dated September 12, 2002. | Additional requirements for processing applications of Stock Brokers for Registration/ Prior approval for sale of membership/ Change of name/ trade |

| | | |
|---|---|---|
| | | name. |
| 16. | SEBI/SMD/SE/15/2003/29/04 dated April 29, 2003 | Issuance of Contract Notes in electronic form |
| 17. | SMD/DBA-II/Cir-16/9618/03 dated May 05, 2003. | SEBI Registration Number of Brokers / Sub-Brokers to be quoted on all correspondences with SEBI. |
| 18. | SEBI/MIRSD/CIR-06/2004 January 13, 2004. | Review of norms relating to trading by Members/Sub-Brokers. |
| 19. | MIRSD/DR-1/CIR-16/09 dated November 06, 2009. | Market Access through Authorised Persons. |
| 20. | MIRSD/SE/CIR-19/2009 dated December 03, 2009. | Dealings between a client and a stock broker (trading members included). |
| 21. | SEBI/MIRSD/MASTER CIR-04/2010 dated March 17, 2010. | Master Circular on Oversight of Members (Stock Brokers/Trading Members/Clearing Members of any Segment of Stock Exchanges and Clearing Corporations). |
| 22. | SEBI/CIR/MIRSD/AP/8/2010 dated July 23, 2010. | Market Access through Authorised Persons. |
| 23. | CIR/MIRSD/9/2010 dated November 04, 2010. | Display of Details by Stock Brokers (including Trading Members). |
| 24. | SEBI/MIRSD/CIR/01/2011 dated May 13, 2011. | Clarification on circular dated December 3, 2009 on 'Dealings between a Client and a Stock broker. |
| 25. | CIR/MIRSD/2/2011 dated June 03, 2011. | Periodical Report – Grant of prior approval to members of Stock Exchanges/Sub-Brokers. |
| 26. | CIR/MIRSD/03/2011 dated June 09, 2011. | Pre- funded instruments / electronic fund transfers. |
| 27. | CIR/MIRSD/12/2011 dated July 11, 2011. | Clarification regarding admission of Limited Liability Partnerships as Members of Stock Exchanges. |
| 28. | CIR/MIRSD/15/2011 dated August 02, 2011. | SMS and E-mail alerts to investors by Stock Exchanges. |
| 29. | CIR/MIRSD/16/2011 dated August 22, 2011 | Simplification and Rationalization of Trading Account Opening Process |
| 30. | CIR/MIRSD/18/2011 dated August 25, 2011. | Redressal of investor grievances against Stock Brokers and Sub-Brokers in SEBI Complaints Redress System (SCORES). |

| | | |
|---|---|---|
| 31. | MIRSD/SE/CIR-21/2011 dated October 05,2011. | Uniform Know Your Client (KYC) requirements for the securities market |
| 32. | CIR/MIRSD/24/2011 dated December 15, 2011 | Guidelines on Outsourcing of Activities by Intermediaries |
| 33. | CIR/MIRSD/13/2012 dated December 07, 2012. | Oversight of Members (Stock Brokers/Trading Members/Clearing Members of any segment of Stock Exchanges/Clearing Corporations). |
| 34. | CIR/MIRSD/5/2013 dated August 27, 2013. | General Guidelines for dealing with Conflicts of Interest of Intermediaries, Recognised Stock Exchanges, Recognised Clearing Corporations, Depositories and their Associated Persons in Securities Market. |
| 35. | CIR/MIRSD/13/2013 dated December 26, 2013 | Know Your Client Requirements |
| 36. | CIR/MIRSD/2/2014 dated June 30, 2014. | Inter-Governmental Agreement with United States of America under Foreign Accounts Tax Compliance Act – Registration. |
| 37. | CIR/MIRSD/3/2014 dated August 28, 2014. | Information regarding Grievance Redressal Mechanism. |
| 38. | CIR/MIRSD/4/2014 dated October 13, 2014. | Single registration for Stock Brokers & Clearing Members. |
| 39. | CIR/MIRSD/2/2015 dated August 26, 2015. | Implementation of the Multilateral Competent Authority Agreement and Foreign Account Tax Compliance Act. |
| 40. | CIR/MIRSD/3/2015 dated September 10, 2015. | Reporting Requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) – Guidance Note. |
| 41. | CIR/MIRSD/4/2015 dated September 29, 2015. | Registration of Members of Commodity Derivatives Exchanges. |
| 42. | CIR/MIRSD/64/2016 dated July 12, 2016 | Simplification of Account Opening Kit |
| 43. | CIR/MIRSD/66/2016 dated July 21, 2016 | Operationalisation of Central KYC Records Registry (CKYCR) |
| 44. | SEBI/HO/MIRSD/MIRSD2/CIR/P/2016/92 dated September 23, 2016. | Regulatory Framework for Commodity Derivatives Brokers. |

| | | |
|---|---|---|
| 45. | SEBI/HO/MIRSD/MIRSD2/CIR/P/2016/95 dated September 26, 2016. | Enhanced Supervision of Stock Brokers/Depository Participants. |
| 46. | SEBI/HO/MIRSD/MIRSD6/CIR/P/2017/20 dated March 10, 2017. | Redressal of complaints against Stock Brokers and Depository Participants in SEBI Complaints Redress System (SCORES). |
| 47. | SEBI/HO/MIRSD/MIRSD1/CIR/P/2017/38 dated May 02, 2017. | Online Registration Mechanism for Securities Market Intermediaries. |
| 48. | CIR/HO/MIRSD/MIRSD2/CIR/P/2017/64 dated June 22, 2017. | Clarification to Enhanced Supervision Circular. |
| 49. | CIR/HO/MIRSD/MIRSD2/CIR/P/2017/73 dated June 30, 2017. | Policy of Annual Inspection of Members by Stock Exchanges/Clearing Corporations. |
| 50. | SEBI/HO/MIRSD/MIRSD1/CIR/P/2017/104 dated September 21, 2017. | Integration of broking activities in Equity Markets and Commodity Derivatives Markets under single entity. |
| 51. | CIR/HO/MIRSD/MIRSD2/CIR/PB/2017/107 dated September 25, 2017. | Clarification to Enhanced Supervision Circular. |
| 52. | SEBI/HO/MIRSD/MIRSD2/CIR/P/2017/123 dated November 29, 2017. | Modification to Enhanced Supervision Circular. |
| 53. | SEBI/HO/MIRSD/DOP1/CIR/P/2018/54 dated March 22, 2018. | Circular on Prevention of Unauthorised Trading by Stock Brokers. |
| 54. | SEBI/HO/MIRSD/DOP/CIR/P/2018/113 dated July 12, 2018 | Discontinuation of acceptance of cash by Stock Brokers |
| 55. | SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 | Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants |
| 56. | SEBI/HO/MIRSD/DOP/CIR/P/2018/153 dated December 17, 2018 | Early Warning Mechanism to prevent diversion of client securities |
| 57. | SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019 | Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries |
| 58. | SEBI/HO/MIRSD/DOP/CIR/P/2019/14 dated January 11, 2019 | Uniform membership structure across segments |
| 59. | CIR/HO/MIRSD/DOS2/CIR/PB/2019/038 dated March 15, 2019 | Clarification to Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants |

| | | |
|---|---|---|
| 60. | CIR/HO/MIRSD/DOP/CIR/P/2019/75 dated June 20, 2019 | Handling of Clients' Securities by Trading Members/Clearing Members |
| 61. | SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019 | Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants-Clarifications |
| 62. | SEBI/HO/MIRSD/DOP/CIR/P/2019/136 dated November 15, 2019 | Mapping of Unique Client Code (UCC) with demat account of the clients |
| 63. | CIR/HO/MIRSD/DOP/CIR/P/2019/139 dated November 19, 2019 | Collection and reporting of margins by Trading Member(TM) /Clearing Member(CM) in Cash Segment |
| 64. | SEBI/HO/MIRSD/DOP/CIR/P/2020/28 dated February 25, 2020 | Margin obligations to be given by way of Pledge/ Re-pledge in the Depository System |
| 65. | SEBI/HO/MIRSD/DOP/CIR/P/2020/88 dated May 25, 2020 | Implementation of Circular on 'Margin obligations to be given by way of Pledge / Re-pledge in the Depository System' - Extension |
| 66. | SEBI/HO/MIRSD/DPIEA/CIR/P/2020/115 dated July 01, 2020 | Standard Operating Procedure in the cases of Trading Member / Clearing Member leading to default |
| 67. | SEBI/HO/MIRSD/DOP/CIR/P/2020/146 dated July 31, 2020 | Collection and Reporting of Margins by Trading Member (TM) / Clearing Member (CM) in Cash Segment |
| 68. | SEBI/HO/MIRSD/DOP/CIR/P/2020/158 dated August 27, 2020 | Execution of Power of Attorney (PoA) by the Client in favour of the Stock Broker / Stock Broker and Depository Participant |
| 69. | SEBI/HO/MIRSD/DOP/CIR/P/2020/173 dated September 15, 2020 | Collection and Reporting of Margins by Trading Member (TM) / Clearing Member (CM) in Cash Segment - Clarification |
| 70. | SEBI/HO/MIRSD/DPIEA/CIR/P/2020/186 dated September 28, 2020 | Recovery of assets of defaulter member and recovery of funds from debit balance clients of defaulter member for meeting the obligations of clients / Stock Exchange / Clearing Corporation |
| 71. | SEBI/HO/MIRSD2/DOR/CIR/P/2020/221 dated November 03, 2020 | Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions |
| 72. | SEBI/HO/MIRSD/DOC/CIR/P/2020/226 dated November 06, 2020 | Investor Grievance Redressal Mechanism |

| | | |
|---|---|---|
| 73. | SEBI/HO/MIRSD/DOP/CIR/P/2021/31 dated March 10, 2021 | Rollout of Legal Entity Template |
| 74. | SEBI/HO/MIRSD/DOR/CIR/P/2021/42 dated March 25, 2021 | Prior Approval for Change in control: Transfer of shareholdings among immediate relatives and transmission of shareholdings and their effect on change in control |
| 75. | SEBI/HO/MIRSD/DOR/CIR/P/2021/46 dated March 26, 2021 | Transfer of business by SEBI registered intermediaries to other legal entity |
| 76. | SEBI/HO/MIRSD/DOP/P/CIR/2021/577 dated June 16, 2021 | Settlement of Running Account of Client's Funds lying with Trading Member (TM) |
| 77. | SEBI/HO/MIRSD/DOP/P/CIR/2021/595 dated July 16, 2021 | Block Mechanism in demat account of clients undertaking sale transactions |
| 78. | SEBI/HO/MIRSD/DOP/CIR/P/2021/653 dated October 28, 2021 | Maintenance of current accounts in multiple banks by Stock Brokers |
| 79. | SEBI/HO/MIRSD/MIRSD_IT/P/CIR/2021/0000000658 dated November 16, 2021 | Framework for Regulatory Sandbox |
| 80. | SEBI/HO/MIRSD/DOP/CIR/P/2021/676 dated December 02, 2021 | Publishing Investor Charter and disclosure of Investor Complaints by Stock Brokers on their websites |
| 81. | SEBI/HO/MIRSD/DoP/P/CIR/2022/44 dated April 04, 2022 | Execution of 'Demat Debit and Pledge Instruction' (DDPI) for transfer of securities towards deliveries / settlement obligations and pledging / re-pledging of securities |
| 82. | SEBI/HO/MIRSD/DoR/P/CIR/2022/61 dated May 13, 2022 | Guidelines for seeking NOC by Stock Brokers / Clearing Members for setting up Wholly Owned Subsidiaries, Step Down Subsidiaries, Joint Ventures in GIFT IFSC |
| 83. | SEBI/HO/MIRSD/DPIEA/CIR/P/2022/72 dated May 27, 2022 | Modification to Standard Operating Procedure in the cases of Trading Member / Clearing Member leading to default |
| 84. | SEBI/HO/MIRSD/DOS3/P/CIR/2022/78 dated June 03, 2022 | Investor Redressal Grievance Mechanism |
| 85. | SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 | Modification in Cyber Security and Cyber resilience framework for Stock Brokers / |

| | | |
|---|---|---|
| | | Depository Participants |
| 86. | SEBI/HO/MIRSD/ MIRSD_DPIEA/P/CIR/2022/83 dated June 20, 2022 | Naming / Tagging of demat accounts maintained by Stock Brokers |
| 87. | SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 | Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants |
| 88. | SEBI/HO/MIRSD/DoP/P/CIR/2022/101 dated July 27, 2022 | Settlement of Running Account of Client's Funds lying with Trading Member (TM) |
| 89. | SEBI/HO/MIRSD/DoP/P/CIR/2022/109 dated August 18, 2022 | Block Mechanism in demat account of clients undertaking sale transactions |
| 90. | SEBI/HO/MIRSD/DOP/P/CIR/2022/117 dated September 02, 2022 | Performance/return claimed by unregulated platforms offering algorithmic strategies for trading |
| 91. | SEBI/HO/MIRSD/DoP/P/CIR/2022/119 dated September 19, 2022 | Validation of Instructions for Pay-In of Securities from Client demat account to Trading Member (TM) Pool Account against obligations received from the Clearing Corporations |
| 92. | SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/137 dated October 06, 2022 | Execution of 'Demat Debit and Pledge Instruction' (DDPI) for transfer of securities towards deliveries / settlement obligations and pledging / re-pledging of securities-Clarification |
| 93. | SEBI/HO/MIRSD/DOP/P/CIR/2022/143 dated October 27, 2022 | Block Mechanism in demat account of clients undertaking sale transactions-Clarification |
| 94. | SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/153 dated November 11, 2022 | Handling of Clients' Securities by Trading Members (TM)/ Clearing Members (CM) |
| 95. | SEBI/HO/MIRSD/DoP/P/CIR/2022/162 dated November 25, 2022 | Extension of timelines for implementation of SEBI circulars SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/137 and SEBI/HO/MIRSD/DoP/P/CIR/2022/119 |
| 96. | SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022 | Framework to address the 'technical glitches' in Stock Brokers' Electronic Trading Systems |

| | | |
|---|---|---|
| 97. | SEBI/HO/MIRSD/MIRSD-PoD-2/P/CIR/2022/163 dated November 28, 2022 | Procedure for seeking prior approval for change in control |
| 98. | SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/177 dated December 30, 2022 | Introduction of Investor Risk Reduction Access (IRRA) platform in case of disruption of trading services provided by the Trading Member (TM) |
| 99. | SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/24 dated February 06,2023 | Enhanced obligations and responsibilities on Qualified Stock Brokers (QSBs) |
| 100. | SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/30 dated February 15, 2023 | Maintenance of a website by stock brokers and depository participants |
| 101. | SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/42 dated March 27, 2023 | Nomination for Eligible Trading and Demat Accounts –Extension of timelines for existing account holders |
| 102. | SEBI letter dated June 24, 2008 | SEBI letter number MRD/DoP/NSE/129791/2008 |
| 103. | SEBI letter dated March 31, 2015 | SEBI letter number MRD/DMS/OW/9500/2015 |
| 104. | Email dated April 13, 2022 | Issuance of Electronic Contract Notes (ECN) through SMS/electronic instant messaging services |