POLICY FOR INTERNAL CONTROL POLICY & PROCEDURES

Policy created by: Anand Jain

Policy reviewed by: Madhulika Jain

Policy reviewed on: 11th May 2026

Policy approved by: Board of Directors

Policy approved on: 11th May 2026

1. Introduction

K.M.Jain Stock Brokers Pvt Ltd (hereinafter referred to as the 'COMPANY') a body corporate , registered under the provisions of the Companies Act 1956, is a SEBI registered broker of the National Stock Exchange of India Ltd. (NSE), Bombay Stock Exchange Ltd (BSE), Metropolitan Stock Exchange and Depository participant of CDSL.

The company has adopted various policies & procedures for internal control measures & tools for compliance of various Acts, rules & regulations of the Exchanges/Depositary.

A. CLIENT REGISTRATION POLICY

New account opening form containing Rights and obligation documents, Risk Disclosure Document, Guidance for DO's and Don'ts for trading on Exchange, Policies & Procedure must be signed by the client. The client may or may not sign the Voluntary documents.
The required documents should be collected from the clients strictly as per the documents mentioned in the checklist of the agreement book.

- Thorough checking by back office in charge including in-person verification, tallying the supporting documents with the original and interview of client.

- After Signature of the Director on behalf of KNA the new Client Code is allotted

- Uploading the client details to the NSE/BSE/MSEL/CSDL

- On receipt of Valid Report, accompanying the codes allocated to clients the same is intimated over telephone and Welcome Letter along with photocopy of KYC along with documents received from the client is send to the client.

- The KRA duly filled with supporting documents is sent to KRA agency

- The KYC Filing of Client Registration Kit & updation of Index

- Periodical Review of financial data

- Deactivation of Client Code on receipt of written documents from Client.

- Intimation in writing to Client regarding deactivation of client code & reason thereof

- Financial capability of the clients is assessed depending on their turnover and is assessed at the end of each financial year. For this KNA ensures to update the financial information of the active clients. Financial statements for all corporate clients who are active are collected.

Walk in Clients: The company has decided not entertain Walk in Clients. All clients / would be Clients are required to submit proper references or introducers.

Financial Documentation: All clients are required to submit updated financial data, namely, their Balance Sheet, Salary Income Certificate. Incase of re-activation of UCC, the clients are also required to submit written request. Clients, specially operating in F&O Segment are compulsorily required to submit their latest financial position every year without fail.

Maker & Checker Concept: The Company appoints different person for checking CRF/data submitted by client and data entered in computer for uploading to master file & the Exchanges. Even after uploading of data, the compliance officer checks the data entered from the CRF. All blank spaces in the CRF is crossed by the compliance officer, if found not crossed by the client.

Marketing Division: The Company does not have any marketing Division

Closure of Client Accounts/ Dormant Accounts: Clients accounts are closed either by client himself or action initiated by the company. On receipt of written request from the client, the compliance officer deactivates the client code in its front & back office. CRF form is marked closed only after proper verification of client's ledger account & clearance received from accounts department regarding dues & margin. Moreover written communication is also sent to client accompanying closure of his account.

Client's accounts are also closed on action initiated by the company in the following cases:

a. If client fails to meet his obligation within stipulated time or time provided by the company

b. If clients fails to provide proper documents as required under SEBI rules & regulations even after repeated request by the company.

c. If client is declared fugitive under any law in India or abroad.

d. If client is declared insolvent under any law in India or any criminal cases are filed or pending and such information is not disclosed at the time of registration with the company

The company also mark all inoperative client account as 'dormant' till the same is closed or reactivated after written request is received from the client. UCC allotted to closed account is not used for any other new client.

B. TRADING POLICY:

Active Client master list should be uploaded in the NEAT/Fast Trade Plus trading terminal and all the orders from the clients should be checked for the client codes in the list. This will ensure minimal wrong code punching by the dealers.

Dealers should be vigilant in executing the orders of the client. They should check & report to senior authorities / Compliance Officer if any client is giving order of abnormal quantity or rates.

Every client should be contacted after the market hours for trade confirmation. The clients should be asked for the settlement of their obligation before settlement date of the exchange.

Every client must be attended by the staff allocated for the purpose and in his absence; compliance officer must ensure that client is attended by another dealer. Staff/ dealer should check the margin availability/credit limit of the client before executing any trade on his behalf.
No trades will be transferred to code other than entered in trading terminal after trading hours unless there is genuine mistake on part of the dealer of client mentioning the UCC at the time of placing the order. Transfer of code can be done only by the 'compliance officer' during the allowable time frame by the exchange on system provided by it.
This step will help us to trace any discrepancies in the trade as well as timely receipt of cheques and securities from the clients and provide better service.

Contract Notes, Daily Margin Statement, Quarterly Statements of Accounts and Register of Securities to Clients

1. All Contract Notes are physically/electronically sent and we are in the process of implementing E-Contract within 24 hours from the trading date.

2. In addition to Contract Notes Daily Margin Statement is dispatched to the clients within 24 hours. The clients are informed about their margin details with breakups in the form of Cash, FDR, BG securities in the daily margin statement sent to them.

3. Contract Notes, Daily Margin Statements, Quarterly Statements of Accounts and Register of Securities are all sent to clients in Physical Form.

4. Contract Notes, Daily Margin Statements, Quarterly Statements of Accounts and Register of Securities are issued by the Head Office, irrespective whether the trade has been executed at the head office or at the branch office. The company follows centralized system of accounting and as such all documents relating to the clients are issued to the client from head office.

5. Till Date we have not yet implemented sending documents via email.

6. All the documents dispatched to the client can be easily retrieved from the software. Further backup of all documents sent is kept separately to avoid any type of inconvenience.

C. PAYMENT POLICY:

1. Payments to clients shall be made on Pay out basis i.e within 24 hours of pay out (T or T+1 day- as applicable).

2. For clients who are desirous of keeping the pay out money with us as margin money can do so by submitting a letter to that effect mentioning therein not to issue cheques until a written request is made. However, such request at a time will be valid for one financial year only and/or until the same in being revoked by the client as the case may be.

3. For clients who are desirous of keeping the pay out money with us for future transactions can do so by submitting a letter to that effect mentioning therein to keep their account as 'running

account' and periodical cheques may be paid or received. However, the clients are required to neutralize and settle their account once in ever one/three months of first transaction.

4. Clients, who have debit balance in one segment and credit balance in other segment, will be paid only if their net balance is credit.

5. Margin Money to the clients will be returned only after adjusting debit balance, if any, in their account and/or if they have not defaulted in their obligation to deliver shares/securities.

6. Payments to the clients will be directly deposited in their account if mandate is given by them to this effect and they have account in the same bank, where the company has its account.

D. RECEIPT POLICIES

1. Cheques from clients would be accepted only of those banks whose details have been provided during client registration.

2. No third party cheques would be accepted.

3. NO CASH PAYMENT IS ACCEPTED.

4. Clients are advised not deposit any cash/cheque directly to company's account. If cheque is deposited then intimation should be given in writing along with pay in slips otherwise credit will not be given to client till proper documents are received from client.

5. Local Cheques received within 2 PM will be posted to the ledger on the same day. The effect of the cheques received beyond 2 PM would be given on the next day.

6. While receiving RTGS / NEFT from client it must be ensured that the same has been received from clients registered account only. Proper record of the UTR number should be maintained.

E. PRE-FUNDED INSTRUMENTS POLICY

Objective:
The objective of the policy is to prevent acceptance of third party funds and to prescribe process to deal with instruments issued by third party when received.

Background:
SEBI vide circular no. SEBI/MRD/SE/Cir-33/2003/27/08 dated August 27, 2003 has specified that the stock brokers can accept demand drafts from their clients. However, SEBI vide circular no. CIR/MIRSD/03/2011 dated June 9, 2011 and National Stock Exchange vide its circular no. NSE/INSP/18024 dated 09-Jun-11 has advised stock brokers to maintain an audit trail while receiving funds from the clients through Demand Draft (DD)/Pay Order (PO)/Bankers Cheque (BC) since such third party pre-paid instruments do not contain the details like name of the client, bank account number are not mentioned on such instruments. Non maintenance of audit trail may result

in flow of third party funds or unidentified money which may result into breach of regulations issued under PMLA and SEBI circulars.

Terms used in this policy:

1. **Prefunded Instruments** - Referred as Pay order, Demand Draft, banker's cheque etc.
2. **Electronic Fund Transfers -** Referred as transfer of funds using net banking

Policy:

SEBI vide circular no. SEBI/MRD/SE/Cir-33/2003/27/08 dated August 27, 2003 has specified that the stock brokers can accept demand drafts from their clients. However, in accordance with SEBI circular no. CIR/MIRSD/03/2011 dated June 9, 2011, the following needs to be complied:

1. A "Pre-paid instrument received register" with columns for date, name of the client, amount, instrument drawn on (bank name) and such other columns as found necessary shall be maintained. The register may be maintained either in a physical form or in electronic form.

2. Pre-paid instruments of the value of less than Rs 50,000 may be accepted from the client. Whenever such instruments are received, entry into 'Pre-paid instruments Received register shall be made.

3. If the pre-paid instrument is for value more than Rs 50,000 or If the aggregate value of prefunded instruments is Rs. 50,000/- or more, per day per client is presented for acceptance, such instrument or instruments may be accepted, only if the same is/are accompanied by the name of the bank account holder and number of the bank account debited for the purpose, duly certified by the issuing bank. The mode of certification may include the following:

I. Certificate from the issuing bank or its letter head or on a plain paper with the seal of the issuing bank.

II. Certified copy of the requisition slip (portion which is retained by the bank) to issue the instrument.

III. Certified copy of the passbook / bank statement for the account debited to issue the instrument.

IV. Authentication of the bank account-number debited and name of the account holder by the issuing bank on the reverse of the instrument.

4. If a client submits pre-paid instruments at different times during the day, details and certificates as stated above may be collected along with the instrument with which the aggregate value of pre-paid instruments submitted exceeds Rs 50,000 for that date.

5. In case of any receipt of funds by way of Electronic fund transfer, an audit trail to ensure that funds are received from respective client only has to be maintained. Necessary details may be collected from banker at which the amount is received.

6. If the pre-paid instrument is received through post or any other method where client does not directly interface for submission of the instrument and the instrument does not contain the information as required above, the following action may be taken:

- Contact the client immediately and seek information. Not to bank the instrument until the

information is given by the client.
- If the pre-paid instrument is bank transfer, contact banker immediately for the details; not utilize the amount so credited until the details are received and not to give credit to the customer until banker gives the details/certification.

7. While giving credit to respective client's ledger, Head office needs to cross check / verify with documents that such instrument is received from respective clients.

Approval Authority:

This policy shall be approved by Board of Directors of K M Jain Stock Brokers Pvt Ltd

Review Policy:

This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs. The policy may be reviewed by our Designated Directors, who can place the changes in policy before the Board at the meeting first held after such changes are introduced.

Policy communication:

A copy of this policy shall be made available to all the relevant staff who are responsible for receipt of funds from clients and customer service executives.

Disclaimer: From time to time this policy will be made more comprehensive based on our business requirements and this may not be treated as the full and final policy. Reference circulars of any other exchange might be added as and when required.

F. MARGIN POLICY

<u>SEGMENT – F&O (NSE AND BSE)</u>

- In the F&O segment, it is mandatory to collect SPAN margin & Extreme loss margin from respective clients on an upfront basis. We will ensure that all upfront margins are collected in advance of trade.
- Collected margin should be allocated in NMASS in respective client UCC code.
- In the equity derivative segment, we will accept approved securities from clients for margin.
- For overnight F&O positions, 50% of the margin should be compulsorily come in cash and the remaining 50% can be in terms of collateral margin.
- Liquid funds include Cash, FDs, GSec, T-Bills and LiquidBeEs. 50% rule wouldn't apply to liquid funds. We encourage our clients to opt for T-Bills, Liquid Bees and G-Sec over FDs.
- Margin received from pledging above will be equivalent to cash in your trading account.
- We shall accept collateral from clients in the form of securities, only by way of 'margin pledge', created in the Depository system.
- Margin collection and reporting, shall compute on the value of such securities as per the closing rate on T-1 day as reduced by the appropriate haircut at a rate not less than the VAR margin rate of the security on that day i.e. T-1 day.
- Cheques received by us for M2M on or before T and deposited by T+1 day (excluding bank holiday, if any), can be considered, provided the same is cleared within T+5 working days.
- Only cheques that are cleared will be considered and while dishonored cheques or un-cleared up to T+5 working days will not be reported as margin/ margin on consolidated crystallized obligation/ MTM collected.

Reporting of margin in FO segment

- We will provide margin reports to clients on daily basis at the end of the trade day (T-Day) itself or by such timelines as may be specified from time to time . Margin pledge collaterals have to be mentioned in the daily margin statement. The indicative format of Daily Margin Statement to be issued to client is as per Annexure B of the Exchange Circular number NSE/INSP/45191 dated July 31, 2020

- Collection of M2M LOSS in FO segment

- Cheques received by us for M2M on or before T day and deposited by T+1 day (excluding bank holiday, if any), can be considered, provided the same is cleared within T+5 working days.
- Penalty levied by clearing corporations of short/non-collection of upfront margins may be passed on to client only if short/non-collection of upfront margin is on account of the following reasons attributable to the client:
    a) No penalty to the client for short allocation of upfront margin

    b) Cheques issued by client to broker is dishonored for M2M

Summary:

T day rule to be followed for upfront margin / VAR / ELM /MTM

For MTM, client's cheque may be accepted with the condition that it should be cleared on T+5 basis.

Upfront Margin/Exposure Margin- Mandatory to be collected; can be 100% cheque or in the ratio 50:50 if the client opts to give securities as collateral

VAR margin- to be given on T DAY basis

MTM margin- to be given on T basis; if the client gives a cheque then it should be cleared on T+5 basis

Collateral and haircut - As per exchange guidelines T-1 day value and VAR file

SEGMENT – CASH SEGMENT (NSE AND BSE)

- In the capital market segment- 20% upfront margin to be collected mandatorily and upfront, in lieu of VaR and ELM from the client on an upfront basis other than T2T(TRADE FOR TRADE).

- Other margins such as Mark-to-market margin (MTM), delivery margin, special/additional margin, or such other margins as may be prescribed from time to time, shall be collected within 'T+0' working days from their clients and allocation made in NMASS of NSCCL for respective UCC code. It must be ensured that a minimum 20% upfront margin is collected in advance before trade execution and other margins are collected/paid as soon as margin calls are made by the clearing corporations.

- For margin collection and reporting purpose points we credit for sale of shares by a client to be considered for which an early pay-in (EPI) request via Block mechanism has been accepted by depositories. The same may be considered as margin collected towards peak margin for the said sale transaction. The sale value of up to 100% of such securities (EPI value) shall be available as a Margin for other positions across all the segments.
- Early pay-in of securities (by block mechanism) /funds made by the clients to the trading broker will be treated as an upfront margin.

<u>Collection/reporting of in Cash segment</u>

- Margin collection and reporting, shall be computed on the value of such securities as per the closing rate on T-1 day as reduced by the appropriate haircut at a rate not less than the VAR margin rate of the security on that day i.e. T-1 day.

- We will provide margin reports to clients daily at the end of the trade day (T Day) itself or by such timelines as may be specified from time to time.

<u>Towards collection/reporting of MTM losses (in Cash Segment)</u>:

- Cheques received / recorded in the books of clients' ledger towards margin daily at the end of the trade day (T Day) itself or by such timelines as may be specified from time to time

- Penalty levied by clearing corporations of short/non-collection of upfront margins may be passed on to the client if short/non-collection of upfront margin is on account of the following reasons attributable to the client:
    I. No- for upfront margin

    II. In case a Cheque issued by the client for M2M OR PAYIN is dishonored.

Summary:

T+0 day margin obligation and T+1 rule to be followed for pay-in obligations

Upfront Margin/Exposure Margin/VAR margin- Normally clients are asked to pay margin amount upfront.

MTM margin- Normally clients are asked to pay according to their pay-in obligations

Collateral and haircut- As per exchange guidelines T-1 day value and VAR file.

Guidelines/clarifications on Margin collection & reporting

In view of the SEBI circular SEBI/HO/MRD/DRMNP/CIR/P/2018/75 dated May 02, 2018 on "Additional Risk management measures for derivatives segment" and NSCCL circulars NSCCL/CMPT/37751 & NSCCL/CD/37750 dated May 14, 2018, Exchange has issued revised guidelines/clarification on Margin collection & reporting and as per guidelines issued by Exchange and SEBI from time to time

The key changes are as under:

a) Reporting of MTM losses

b) Collection of MTM loss by T day.

c) Collaterals in cash collected for upfront margin can be considered towards collection of MTM losses.

d) Trading Member or its associate company is a Depository Participant and POA for considering securities towards margins as by way of pledge is in favor of Trading Member,

The key changes are as under:

a) Reporting of MTM losses

b) Collection of MTM loss by T day.

c) Collaterals considered in cash towards upfront margin can be considered towards collection of MTM losses.

Penalty structure in case of short margin received from clients and reporting:

Penalty levied by clearing corporations of short/non-collection of upfront margins may be passed on to client only if short/non-collection of upfront margin is on account of the following reasons attributable to the client:

- No penalty to the client for short allocation of upfront margin
- Cheque issued by client to broker is dishonored for M2M

a) The records should be periodically reconciled with the actual collateral deposited with the broker.

REGULATORY REQUIREMENTS; 1	Clarification regarding margin collection and reporting by members	Circular Ref. No.: 126/2011, download Ref. No.: NSE/INSP/19583 dated December 14, 2011; Download Ref. No.: NSE/INSP/24805; Circular Ref No.: 168/2013 dated October 23, 2013; SEBI/HO/MRD/DRMNP/CIR/P/ 2018/75 dated May 02, 2018; Circular Ref. No.: 331/2018, download Ref. No.: NSE/INSP/38154 dated June 27, 2018 Latest available on NSE INDIA.COM under the FAQS of Margin collection and Reporting
2	Daily Margin Statement Format	Circular Ref.No.: 126/2011, download Ref. No.: NSE/INSP/19583 dated December 14, 2011; Download Ref. NSE/INSP/36786 dated January 19, 2018; Circular Ref. No.: 331/2018, download Ref. No.: NSE/INSP/38154 dated June 27, 2018 , NSE/INSP/45191 dated July 31, 2020
3	Collateral deposited by clients with members	Circular no. NSE/INSP/2008/66, download reference no. NSE/INSP/10605 dated 21st April 2008, NSE/INSP/45191 dated July 31, 2020
4	FAQs on Margin Collection and Reporting	Download Ref. No.: NSE/INSP/25612; Circular Ref No.: 177/2014 dated January 20, 2014; Download Ref. No.: NSE/INSP/38154; Circular Ref. No.: 331/2018 dated June 27, 2018 (supersedes the old circular with download ref no. NSE/INSP/25612) Latest available on NSE INDIA.COM under the FAQS of Margin collection and Reporting

G. SECURITIES

Collection of securities

1. To ensure that clients are delivering the shares from their own account and all the deliveries to/from the clients correspond with the details provided by the client with their registration.

2. The statement should be checked with the securities obligation of the clients. Any third party delivery from the clients should not be delivered to clearing house.

3. No credit to clients should be given even though shares received from third party has been delivered to clearing house due to any technical reasons beyond management's control. If client provides sufficient written proof of ownership of such account/share, than after updating client database, client may be given effect of the same.

4. The reports provided by Exchange should be used to check whether there is any short pay-in/ out of securities to/from Clearing house.

Delivery of Securities

1 The company will be making direct pay-out of shares to client account of which details are given in Client Registration Kits.

2. The direct pay-out file should be created by the back office software.

3. The instruction slip for shares delivery from the Pool account in case of client to client transaction or break delivery from the Clearing house should be signed by directors

4. Pay out shares shall be given to clients only when they have clear balance in their ledger account. (*the clear balance means that cheques issued by clients should have been cleared in bank.)

5. Shares of clients having debit balance will be kept with the company as hold back margin.

6. The hold back margin account will be reviewed twice in a week i.e on Wednesday & Saturday and shares will be credited to the accounts of the client if they have clear balance during the time of periodic review.

7. The value of shares to be kept in the holdback margin shall be to the extent the client is having debit balance calculated after taking hair cut into account i.e if the client is having a debit balance of Rs. 100000/- then the shares of worth Rs 140000/- (approx) will be retained in holdback margin and any excess shares shall be released to the account of the client.

H. **SURVELLIANCE - PMLA ALERTS AND REPORTING**

SURVEILLANCE POLICY AND MONITORING OF TRANSACTIONAL ALERTS - FOR NSE BSE MSEL & CDSL

1. Introduction

K.M.Jain Stock Brokers Pvt Ltd (hereinafter referred to as the Trading Member), a body corporate , registered under the provisions of the Companies Act 1956, is a SEBI registered broker of the National Stock Exchange of India Ltd. (NSE), Bombay Stock Exchange Ltd (BSE), Metropolitan Stock Exchange and Depository participant of CDSL.

The company has adopted Surveillance Policy as mandated by SEBI through the following exchange circulars:
BSE Circular # 20210701-30 dated 01 Jul 2021
NSE Circular # NSE/SURV/48818 452/2021 dated 01 Jul 2021
CDSL Circular # CDSL/OPS/DP/SYSTEM/2021/309 dated 15.7.2021

1. Obligation of Trading Members/CDSL-Depository Participants to frame Surveillance Policy:

Trading member – K.M.Jain Stock Brokers Pvt Ltd, is a broking entity catering to retail and institutional clients besides executing trades under "Pro" book. For effective monitoring, trading member shall frame a surveillance policy keeping in mind different types and combination of services to different types of clients including retail, institutional, HNI through various modes like Call and Trade, Mobile based trading, Internet based trading (through Exchange CTCL platform only),in addition to proprietary trading (excluding Algorithmic trading). The said surveillance policy shall, inter alia, cover the following:

1.1. Generation of suitable surveillance alerts which may be guided by indicative themes (the list is inclusive and not exhaustive) given in Para 2 below as well as for transactional alerts downloaded by the Exchanges. (Transactional alerts downloaded by the Exchange are based on some thresholds or parameters. Trading members will also have its own different thresholds or parameters so as to detect any suspicious trading activity).
1.2. Processing of alerts within 45 days from the date of alerts downloaded by the Exchanges as well as alerts generated at trading member's end.
1.3. Documentation of reasons for any delay in disposition of any of the alerts.
1.4. Suspicious / Manipulative activity identification.
1.5. Framework of appropriate actions that can be taken by the Trading member. In addition to the obligations under Prevention of Money Laundering Act (PMLA), actions may include suspension of the trading activity of the suspect client, or any other action as may be deemed appropriate.
1.6. Record maintenance for the period as stipulated under applicable statutes.

This policy needs to be reviewed on a periodic basis to keep it in line with the market trends.

2. Obligation of Trading Member/ CDSL-Depository Participants to generate additional Surveillance alerts:

In addition to the transactional alerts downloaded by Exchanges, Trading member will also generate appropriate surveillance alerts at our end, to enable us to effectively monitor the trading activity of our clients at our end as per the laid down surveillance policy.
The indicative themes on which trading member may formulate alerts are as under. The trading member also needs to analyze patterns and trends with respect to different themes.
2.1. The indicative themes that will be considered by the Trading Member will be as enumerated below.

2.1.1. Client / group of clients, as identified by the trading member, accounting for a significant percentage of the total trading activity in a scrip / contract as compared to the market.
2.1.2. Client / group of clients with new account or clients dealing after a significant time gap, as identified by the trading member, accounting for significant value /percentage of total trading activity in a scrip / contract as compared to the market.
2.1.3. Client / group of clients dealing frequently in small quantities / minimum market lot in a scrip / contract.
2.1.4. Disproportionate trading activity vs reported income / Net worth.
2.1.5. Frequent changes in KYC submitted by clients.
2.1.6. Based on an announcement by a listed company, identify client / group of clients, having possible direct / indirect connection with a listed company, who have undertaken any suspicious trading activity prior to price sensitive announcement by said listed company.
2.1.7. Client / group of clients having significant selling concentration, in the scrips, forming part of 'For Information list' or 'Current Watch list'. For more details, kindly refer Exchange notice no. 20200830-1 dated August 30, 2020.
2.1.8. Consistency in profit / loss at client / group of clients' levels, rationale for such trading activities. In addition, trading members may also refer details given in Exchange notice no. 20190207-46 dated February 07, 2019.
2.1.9. Significant trading activity in scrips by client who has pledged the shares of same scrip.
2.1.10. In case of concerns of trading activity of a client / group of clients in a scrip, monitoring whether the orders are being placed by respective clients or their authorized representatives and monitoring client's address as per KYC vis-a-vis the dealing office address.
2.2. The indicative themes additionally applicable to Trading Members who are Depository Participants.
2.2.1. Significant trading activity in scrips where client has pledged shares or has significant holding or has frequent off-market transactions.
2.3. The indicative themes additionally applicable to Trading Members who have facility of internet-based trading.
2.3.1. Surveillance / monitoring of IP addresses of clients (including identification of multiple client codes trading from the same location).

The above guidelines are illustrative and should not be construed as exhaustive. Based on circumstances and based on business model and service offered to the clients and for proprietary trading, the trading members shall exercise independent judgment and formulate own alerts and take appropriate actions thereof.

3. Obligation of Trading Members / CDSL-Depository Participants w.r.t. client due diligence:

The following activities required to be carried out by the trading members for client due diligence is being reiterated:
3.1. Trading member is required to carry out the Due Diligence of their client(s) on an on-going basis.
3.2. Trading member shall ensure that, key KYC parameters of the clients are updated on a periodic basis as prescribed by SEBI and latest information of the client is updated in UCC database of the Exchange. Based on available information, the trading member shall establish groups / association amongst clients, inter-alia, to identify multiple accounts / common account / group of clients.

4. Obligation of Trading Members/ CDSL-Depository Participants w.r.t. processing of alerts:

4.1. Trading Member shall obtain trading rationale and necessary documentation including bank statements; demat statements for analyzing / processing the alerts.
4.2. After analyzing the documentary evidences, trading member shall record its observations for such identified transactions of its client / group of clients.

4.3. With respect to the transactional alerts downloaded by the Exchange, trading member shall ensure that all alerts are analyzed and status thereof (Verified & Closed /
Verified & Sent to Exchange) including action taken is updated within 45 days, in the e-BOSS System.
4.4. With respect to the alerts generated at the trading members end, trading members shall report instances with adverse observation, along with details of action taken, to the Exchange within 45 days of the alert generation.

5. Obligation of Compliance officer, Designated Director and Internal Auditor of the Trading Member/ CDSL-Depository Participants:

5.1. The surveillance activities of trading member shall be conducted under overall supervision of its Compliance Officer.
5.2. A quarterly MIS shall be put up to the Designated Director / Partner / Proprietor on the number of alerts pending at the beginning of the quarter, generated during the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with reasons for pendency and action plan for closure. Also, the Designated Director / Partner / Proprietor shall be apprised of any exception noticed during the disposition of alerts.
5.3. Designated Director / Partner / Proprietor would be responsible for all surveillance activities carried out by the trading member.
5.4. Internal auditor of trading member shall review the surveillance policy, its implementation, effectiveness and review the alerts generated during the period of audit. Internal auditor shall record the observations with respect to the same in their report.

6. Obligation of Quarterly reporting of status of the alerts generated by the Trading member:
(For Depository participant's format – refer Annexure II attached)

6.1. Trading member shall provide duly approved status of the alerts on a quarterly basis, in the following format to the Exchange within 15 days from end of the quarter.

A. Status of Alerts generated by the Trading member:

Name of Alert	No. of alerts under process at the beginning of quarter	No. of new alerts generated in the quarter	No. of alerts verified & closed in the quarter	No. of alerts referred to Exchange (*)	No. of alerts pending / under process at the end of quarter

B. (*) Details of alerts referred to the Exchange:

Sr. No.	Date of Alert	Type of Alert	Brief observation and details of action taken	Date referred to Exchange

C. Details of any major surveillance action taken (other than alerts referred to Exchange), if any, during the quarter:

Sr. No.	Brief action taken during the quarter

6.2. Trading member, not having anything to report, needs to submit 'NIL Report' within 15 days from end of quarter.
6.3. The above details shall be uploaded by the trading member on the BSE Electronic Filing System (BEFS) and NSE Member Surveillance Dashboard (MSD) within 15 days from end of the quarter.
6.4. The aforementioned quarterly system of reporting shall be effective from the quarter ending September 2021.

7. Penalty in case of late / non submission of Quarterly Reporting of status:
Trading member should note that in case of late / non submission of quarterly reporting of the alerts generated by the trading member as mentioned in Para 6 above, trading member shall be liable for penalty as given below:

Submission of status report beyond stipulated period Penalty to be imposed
1st instance Rs. 10,000 per day till submission of quarterly report
2nd instance onwards Rs. 20,000 per day till submission of quarterly report
Trading members may note that aforesaid penalty shall be levied on a monthly basis based on slabs as mentioned above and same shall be debited in the monthly bill.

8. Disciplinary Action for non-fulfillment of Surveillance obligation by Trading Members:

8.1. Trading member may note that during investigation / inspection, if it is observed that the member has not fulfilled their surveillance obligations, then appropriate disciplinary action shall be initiated against the concerned trading member.
8.2. Any non-compliance with respect to surveillance obligations which may inter alia include delay in processing of transactional alerts downloaded by the Exchange and repeated instances of delay in reporting of the status of alerts, may result in further disciplinary action as deemed fit in terms of Rules, Bye-laws and Regulations of the Exchange.
8.3. It may further be noted that aforesaid measure does not preclude SEBI / Exchange to take any further action(s), if the facts and circumstances so demand.

The above policy shall be effective from August 01, 2021. For BSE NSE & MSEL

The above policy shall be effective from October 01, 2021. For CDSL- Depository Participants

(Subjected to changes as per the then prevailing regulations, if any)

Annexure I (FOR NSE BSE AND MSEL)

Transactional alerts downloaded by the Exchange to facilitate effective surveillance at the Member end:

S.No	Transactional Alerts	Segment
1	Significant increase in client activity	**Cash/ F&O**
2	Sudden trading activity in dormant account	**Cash/F&O**
3	Clients / Group of Client(s) dealing in common scrips	**Cash/F&O**
4	Clients / Group of Client(s) is concentrated in a few illiquid scrips	**Cash**
5	Clients / Group of Client(s) dealing in scrip in minimum lot size	**Cash**
6	Clients / Group of Client(s) Concentration in a scrip	**Cash/F&O**
7	Circular Trading	**Cash**
8	Pump and Dump	**Cash**
9	Reversal of Trades	**Cash**
		Derivatives
10	Front Running	**Cash**
11	Concentrated position in the Open Interest / High Turnover concentration	**Derivatives**
12	Order book spoofing i.e. large orders away from market	**Cash/F&O**
13	High value transaction	**Cash**
14	SEBI Debarred Entities	**Cash/F&O**
15	TRAI	**Cash/F&O**

Annexure II (FOR CDSL- DEPOSITORY PARTICIPANTS)
Transactional alerts downloaded by the Exchange to facilitate effective surveillance at the Member end:

Sr. No.	Indicative themes:
1	Alert for multiple demat accounts opened with same demographic details: Alert for accounts opened with same PAN /mobile number / email id/ bank account no. / address considering the existing demat accounts held with the DP.
2	Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
3	Frequent changes in details of demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.
4	Frequent Off-Market transfers by a client in a specified period
5	Off-market transfers not commensurate with the income/Net worth of the client.
6	Pledge transactions not commensurate with the income/Net worth of the client.
7	Off-market transfers (High Value) immediately after modification of details in demat account
8	Review of reasons of off-market transfers provided by client for off-market transfers vis-à-vis profile of the client e.g. transfers with reason code Gifts with consideration, frequent transfers with reason code Gifts/Donation to unrelated parties, frequent transfers with reason code off-market sales
9	Alert for newly opened accounts wherein sudden Increase in transactions activities in short span of time and suddenly holding in demat account becomes zero or account becomes dormant after some time.
10	Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by their clients.
11	Dormant Instruction Recd
12	High Value Instruction Recd
13	SEBI Debarred Entities
14	TRAI
15	Instruction from EOW (ECONOMIC OFFENCE WING)
16	Directive of Court Order

Obligation of Quarterly reporting of status of the alerts generated by the Depository participants:
Status of Alerts generated by the Depository:

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

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

Sr. No.	Brief action taken during the quarter

Quarterly reporting format to provide comprehensive overview on the alerts generated by DPs.

Name of Alert	**Opening Balance of alerts at the beginning of the quarter** (A)	**No. of alerts generated during the quarter** (B)	**Total no. of alerts (C= A+B)**	**No. of alerts closed during the quarter (D)**	**Alerts pending at the end of the quarter (E = C-D)**	**Ageing analysis of the alerts pending at the end of the Quarter (since alert generation date) (Segregation of E column)**					**Reason for pendency#**
						< 1 month	**1-2 months**	**2-3 months**	**3-6 months**	**> 6 months**	

Notes forming part of CDSL- Depository Participant's Surveillance Policy:

DPs have to analyze and review these alerts based on facts and verification of relevant documents including income/net worth as provided by BO. Further, DPs are required to exercise their independent judgment and take appropriate action in order to detect any abnormal or suspicious transactions.

Our DPs surveillance policy shall take into account the cognizance of type of clients, number of demat accounts, number of transactions etc. and which shall, inter alia, cover the following:
i. Generation of suitable surveillance alerts which may be guided by indicative themes (the list is inclusive and not exhaustive) given in point B below

ii. Review and disposal of transactional alerts provided by CDSL (Transactional alerts provided by CDSL will be based on some thresholds. DPs may have their own different thresholds or own parameters to generate additional alerts of their own in point I above, so as to detect any suspicious transaction activity).

iii. Disposal of alerts within 30 days from the date of alerts generated at DP end and alerts provided by CDSL.

iv. Reporting to CDSL and other authorities as applicable, in case of any abnormal activity

v. Documentation of reasons for delay, if any, in disposition of alerts.

vi. Framework of appropriate actions that can be taken by the Participant as per obligations under Prevention of Money Laundering Act (PMLA)

vii. Record maintenance for the period as stipulated under applicable statutes

viii. The surveillance policy of the DPs shall be reviewed once in a year

I. INVESTOR REDRESSAL SYSTEM/ MECHANISM

1. The company has a separate manual register for recording all clients related complain either received personally or via post or via email.

2. The company has also designated email ID for sending complains by its investors or clients. The email Id has been disclosed in the KYC Kit sent to all clients at the time of registration as well as is mentioned on the contract note.

3. The company has also kept manual investors complain register at its all branches and the same are verified by the compliance officer or its team of official from time to time.

4. The branch manager is responsible for sending the copy of complain received or written in complain register within 24 hours of the receipt of the complain to compliance officer at head office either personally or via email.

5. On receiving the complaint, the Compliance officer is authorized to dispose off the complaint on its merit and write personally to the client of all action taken by him for satisfaction of the client.

6. If the compliance officer deserves the attention of the higher management or if the compliance officer is unable to dispose off complain to the satisfaction of the client or the exchange or the SEBI, the designated directors are informed of the situation by the compliance officer and all documents are placed before them within seven days of the receipt of the complaint.

7. The designated director's review the pending complains every seven days along with matters needed their attention.

Following is the Escalation Matrix: (For Stock Brokers and Depository Participant)

Escalation Matrix: (For Stock Brokers and Depository Participant)				
Details of	**Contact Person**	**Address**	**Contact No.**	**Email id**
Customer care / Client Servicing	Bhavesh Kathiriya - for Stock Brokers Sarika Manjrekar - for Depository Participant	1306, Marathon Icon, Off G. K Marg, Lower Parel – West, Mumbai - 400 013	022 - 49734185 022 - 49734180	grievances@kmjpl.com
Head of Customer Care / Client Servicing	Mansi Jain	1306, Marathon Icon, Off G. K Marg, Lower Parel – West, Mumbai - 400 013	7304521237	support@kmjpl.com
Compliance Officer	Anand Jain	1306, Marathon Icon, Off G. K Marg, Lower Parel – West, Mumbai - 400 013	022 - 46078213	compliance@kmjpl.com
Chief Executive Officer (CEO)	Madhulika Jain	1306, Marathon Icon, Off G. K Marg, Lower Parel – West, Mumbai - 400 013	022 - 49711153	ceo_compliance@kmjpl.com

Working hours of each escalation level is
(9.30 am to 5.30 pm) - Monday to Friday
(10 am to 3 pm) - Saturday
Closed on every 4th Saturday of the month, Sunday's, Exchange and DP holidays

In absence of response/complaint not addressed to your satisfaction, you may lodge a complaint with :
SEBI at https://scores.sebi.gov.in/
or respective Exchanges/ Depository Participant at
BSE: https://bsecrs.bseindia.com/ecomplaint/frmInvestorHome.aspx
NSE: https://investorhelpline.nseindia.com/NICEPLUS/
MSEI: https://www.msei.in/Investors/Introduction
CDSL: https://www.cdslindia.com/Footer/grievances.aspx

After you've exhausted all the options available for resolving your grievance, if you're still not satisfied with the outcome, you can initiate the dispute resolution process through the ODR Portal https://smartodr.in

Please quote your Service Ticket/ Complaint Ref No. while raising your complaint at SEBI SCORES/Exchange portal/Depository Portal.

J. POLICY ON UNAUTHENTICATED NEWS CIRCULATION

1. Employees / Temporary Staffs / Voluntary Workers etc employed/working in our office shall not be encouraged or they shall not circulate rumors or unverified information obtained from client, industry, any trade or any other sources without verification.

2. Access to BLOGS / Chat Forums / Messenger sites etc. are either restricted under supervision of some responsible employees of the company or access shall not be allowed.

3. Logs for any usage of such BLOGS / Chat Forums / Messenger sites (called by any nomenclature) shall be treated as records and the same should be maintained as specified by the respective Regulations which govern our company.

4. Employees are directed that any market related news received by them either in their official mail / personal mail / Blog or in any other manner, should be forwarded only after the same has been seen and approved by the Compliance Officer of our Company. If nay employee fails to do so he/she shall be deemed to have violated the various provisions contained in SEBI Act/Rules/Regulations etc. and shall be liable for actions. The Compliance Officer shall also be held liable for breach of duty in this regard.

K. NISM VII CERTIFICATION

FOR NSE, BSE, MCX-SX
POLICY ADOPTED FOR OFFICERS IN CRITICAL POSITIONS
(Download Ref.No.: NSE/INSP/27495 Date : September 2, 2014 Circular Ref.No.: 198/2014)
NISM-Series-VII: Securities Operations and Risk Management Certification Examination

As per the said guidelines mentioned in SEBi and Exchange's circulars , persons associated with a registered stock-broker/trading member/clearing member who are involved in, or deal with, any of the below mentioned functions are required to have a valid NISM Series VII Certification:
(a) Assets or funds of investors or clients,
(b) Redressal of investor grievances,
(c) Internal control or risk management, and
(d) Activities having a bearing on operational risk,

In view of the operational difficulties expressed by the Members, in consultation with SEBI and other Exchanges it was decided by SEBI that requirement of passing of **NISM Series VII - Securities Operations and Risk Management Certification** exam would be optional for associated persons handling the basic clerical/elementary functions in the above stated areas and whose work is supervised by NISM Series VII -Securities Operations and Risk Management Certification certified personnel. The broad indicative activities that can be classified as basic elementary level/clerical level are enclosed as **Annexure-A**.
The adherence to the above shall be verified during the inspections and Internal Audits of the Members. Members are requested to take note of the above and ensure compliance by December 31, 2014

As on 11.05.2026 the following officers/staff have cleared NISM VII test for the organization-

1. **Vikash Kuthari** **certificate valid till 06 Jul 2028**
2. **Vishal Ambani** **certificate valid till 23 Jun 2029**
3. **Vinod Gujar** **certificate valid till 23 Jun 2029**

ANNEXURE-A(forming part of Policy for NISM VII certificate

Indicative activities falling under basic elementary level/clerical level

Internal control or risk management

1. Inwarding of collateral's/cheques
2. Person performing maker entries
3. Maker entry in the database

4. Photocopying, printouts, scanning of documents
5. Preparing of MIS
6. Sending of letters/reports to clients, Exchanges, SEBI
7. Attending calls, etc.

Redressal of investor grievances

1. Inwarding of complaints,
2. Seeking documents from clients
3. Person performing maker entries
4. Maker entry in the database
5. Photocopying, printouts, scanning of documents
6. Preparing of MIS
7. Sending of letters/reports to clients, Exchanges, SEBI Updation, data entry, uploading on

L. TECHNICAL GLITCH

POLICY ON PREVENTION OF BUSINESS DISRUPTION DUE TO TECHNICAL GLITHCHES

Download Ref No: NSE/COMP/50610 Date: December 15, 2021 Circular Ref. No: 108/2021

Guidelines for prevention of Business Disruption due to technical glitches & Standard Operating Procedures (SOP) to be adopted by K M Jain Stock Brokers Pvt Ltd upon incident of Technical Glitches.

I. Objective The objective of this guideline is to outline the technology infrastructure and system requirements that we as a member should put in place to prevent any incident of business disruption resulting from technical glitches. These guidelines also prescribe the Standard Operating Procedures (SOP) for reporting of technical glitches by staff of KMJPL (K M Jain Stock Brokers Pvt Ltd), handling business disruption, management of such business disruption, including declaration of disaster and framing of provisions for disciplinary action in case of non-compliance in reporting/inadequate management of business disruption.

II. Definition a) “Technical Glitch” shall mean any malfunction of the systems including malfunction in its hardware or software or any products/services provided by KMJPL, whether on account of any inadequacy or non-availability of infrastructure/ network/ other systems or otherwise, which may lead to business disruption. b) “Business Disruption” shall mean either stoppage or variance in the normal functions /operations of systems of KMJPL, due to a technical glitch, w.r.t login, order placement (including modification & cancellation), order execution, order confirmation, order status, margin updates, risk management, for a continuous period of more than 15 minutes in any segment of the Exchange. National Stock Exchange of India Circular Page 3 of 11

III. Preventive Measures a) We, as a Member should have robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating to securities market and provide seamless service to their clients. b) Exchange and SEBI have, from time to time, prescribed various guidelines and advisory to Members to build resiliency/redundancy in their systems to ensure continuity of services to their clients. Further, Exchange also provides various redundancy options to the Members for connectivity, enabling them to create network resilience, which the Members have been advised to deploy to ensure continuity of their business operations. Members are required to ensure due compliance to the same. c) Further, KMJPL shall be required to comply with the system requirements prescribed under the Stockbroker System Audit Framework as well as the framework for Cyber Security & Cyber Resilience prescribed by SEBI vide its Circular CIR/MRD/DMS/34/2013 dated November 06, 2013, and SEBI/HO/MIRSD/CIR/PB/2018/147 dated Dec 03, 2018, respectively and any other circulars/regulations & guidelines issued by SEBI/Exchange in this regard from time to time. d) Additionally, KMJPL will ensure the following: i. System Controls & Network Integrity 1. Sufficient level of redundancy should be deployed and available at primary site for all critical systems including network and data center infrastructure. National Stock Exchange of India Circular Page 4 of 11 2. As a member, we shall implement and deploy suitable monitoring tools to monitor the data traffic within our organization network and to & from the organization network. ii. Backup and Recovery 1. The response and recovery plan of KMJPL should have plans for the timely restoration of systems affected by incidents of technical glitch. 2. KMJPL should, based in their internal policy, define the Recovery Time Objective (RTO) i.e., the maximum time taken to restore the operations, and the Recovery Point Objective (RPO) i.e., the maximum tolerable period for which data might be lost, for each of their business processes/services. The same should also be informed to the clients by the Members.

IV. Business Continuity Planning (BCP)/Disaster Recovery (DR) In order to ensure that there is continuity of business and stability in operations of KMJPL in case of any technical glitches, so that interest of investors and market at large is not adversely impacted. KMJPL should have an established Business Continuity/DR set up to ensure that there is well defined continuity plan in case of such Business Disruptions. 1. KMJPL shall have a well-documented BCP/ DR policy and plan which will cover the following: a. Identification of all critical operations of the Member and also include the process of informing clients in case of any disruptions. While putting in place the BCP/DR National Stock Exchange of India Circular Page 5 of 11 plan, KMJPL will sufficiently review all potential risks along with its impact on the business. b. Declaration of incident as a “Disaster” viz. timelines etc. and restoration of operations from DR Site upon declaration of ‘Disaster’. 2. KMJPL should have distinct primary and disaster recovery sites (DRS) for technology infrastructure, workspace for people and operational processes. The DRS should be set up sufficiently away (not less than 250 km), from Primary Data Centre (PDC) to ensure that both DRS and PDC are not affected by the same disasters. 3. The declaration of disaster shall be reported in the preliminary report submitted to the Exchange, as specified on section V below. 4. Members should have alternate means of communication including channel for communication for communicating with the clients in case of any disruption. Such communication should be completed within 30 minutes from the time of disruption. 5. Adequate resources (with appropriate training and experience) should be available at the DR Site to handle all operations during disasters. 6. DR drills should be conducted by the Member on a periodic basis not exceeding half yearly basis. Members who do not fall in the above category shall inform all their existing clients within a period of one month from the date of this SOP that they are not required to have a Business Continuity/DR plan under the existing regulatory provisions. Such member shall disclose this information upfront to their new clients at the time of onboarding. National Stock Exchange of India Circular Page 6 of 11

Disaster Recovery Site / Business continuity office of K M Jain Stock Brokers Pvt Ltd

Address: 631, P J Towers, Dalal Street, Fort, Mumbai. 400001

V. Reporting Requirements: KMJPL shall be required to report to the Exchange any technical glitches, resulting in Business Disruption. We shall report the same to the Exchange as under: 1. KMJPL should intimate the Exchange about the incident within 2 hours from the start of the glitch. 2. A preliminary incident report shall be submitted 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. 3. Root Cause Analysis (RCA) of the issue in the format as enclosed in Exhibit-I, to be submitted within 21 working days. The RCA must include details of the incident, time of occurrence and recovery, impact, summary as well as a detailed analysis of the cause of incident, immediate action taken and the long-term plan of action.

For the purpose of the aforementioned reporting, a common dedicated email Id, across all Exchanges, is being provided:

infotechglitch@nse.co.in.

Online Reporting of Technical Glitch Incidents

Ref circular # NSE/COMP/54876 dated December 16, 2022.
Technical Glitch incidents can also be reported to Exchange via ENIT portal w.e.f. April 1, 2024.

Procedure:
New ENIT > Compliance > Technical Glitches > Technical Glitches Submission.

It may be noted that we also need to report the incidents on the dedicated email address common across all Exchanges: infotechglitch@nse.co.

The user manual for submitting the application through online portal is attached as Annexure A in the above notice.

For assistance, please contact the helpdesk at 1800 266 0050 (Select IVR option 3) or email memcompliance_support@nse.co.in

KMJPL shall make the above reporting on the said email ID only. The above reporting requirements shall be applicable to all Members providing internet and wireless technology-based trading facility to their clients. Notwithstanding the above, in case of technical glitches caused by a cyber-security incident, all Members shall also additionally follow the SOP for handling Cyber Security incidents issued vide NSE circular ref. no. NSE/INSP/48163 dated May 03, 2021. National Stock Exchange of India Circular Page 7 of 11 All cases of technical glitches shall be examined by the concerned Exchanges jointly along with the report/RCA submitted by the Member and appropriate action may be taken including suggestion of suitable recommendations for implementation.

VI. Internal Policy and Documentation -All Members, providing internet and wireless technology-based trading facility to their clients shall put in place an Internal policy to handle technical glitches resulting in Business Disruption. Such policy shall: - 1. Outline the key systems/departments handling the normal function /operation of the Member and assign responsibilities at business owner and technology owner level. 2. Lay down the processes/steps to be adopted in case of technical glitches along with the timelines and communication with concerned stakeholders including clients. 3. Define the Escalation matrix including reporting of such incident to the Exchange. 4. The response and recovery plan of the Members for the timely restoration of systems affected by technical glitch including the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). 5. Process of handling client complaints. Refer Such policy shall be approved by Board of the Member (in case of corporate trading member), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and shall be reviewed annually by the “Internal Technology Committee” as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 for review of Security and Cyber Resilience policy or any other appropriate committee in the event that the committee constitution is different for cyber security related issues. National Stock Exchange of India Circular Page 8 of 11 A quarterly MIS shall be put up to the Board, Partners, Proprietor, as the case may be, on incident reported, the corrective actions taken and the future plan of action. Reasons for delay in deployment of the corrective measures shall also be discussed along with the action to be taken. Members shall also constitute a Crisis Management Team (CMT) involving senior officials or management personnel of the members including the

MD/CEO and heads of business, CIO/CTO, CISO, etc. The CMT shall be responsible to assess the incident, oversee the implementation of the corrective and preventive actions and ensure the implementation of the aforementioned procedures. The CMT shall also designate a "Designated Officer" who shall be responsible for ensuring compliance to the aforementioned reporting requirements. The Designated officer can be same as that designated by the Member in accordance with SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated Dec 03, 2018.

VII. Frequency of monitoring & implementation

The aforementioned requirements shall be implemented as per the below timelines: - S.No. Requirements Timeline for implementation

1. Business Continuity Planning (BCP) / Disaster Recovery (DR)	All Members shall, on a quarterly basis, check their eligibility viz. their number of registered clients with respect to setting up the Business Continuity Planning (BCP)/Disaster Recovery (DR) and implement the same as per the below timeline: a) Members having 50000 unique registered clients (across all segments/Exchanges) as on the date of this circular- Within 12 calendar monthsfrom the date of this circular. National Stock Exchange of India Circular Page 9 of 11 b) Other Members - Within 12 calendar months from the end of respective quarter in which the Member becomes eligible as per section IV.
2. Reporting of incident to Exchanges	Immediate basis
3. Internal Policy for Technical Glitch	31st March 2022
4. Preventive Recovery (Para III (a) & III (b) - System Control, Network Integrity, Backup & Recovery)	31st March 2022

VIII. Failure to report the incident to the Exchange (non-submission of preliminary report and/or RCA), failure to move to DR and failure to take remedial measures 1. Delay in Reporting Member will be liable to pay a monetary fine of Rs. 20,000/- for each working day after the due date specified as above for each of the reporting as mentioned in section V above. 2. Repeat Violation In case of repeated instances of non-compliance on 2 or more occasions, appropriate disciplinary action shall be initiated, after following due process and providing opportunity of a hearing. National Stock Exchange of India Circular Page 10 of 11 3. Failure to move to DR site within the timeline timely address specified by the Exchanges/SEBI In the event that Members fail to move to DR site within the time specified, appropriate disciplinary action shall be initiated by the Exchange, after following due process and providing opportunity of hearing. 4. Failure to timely address technical glitch In the event that Members do not address the technical glitch within the timeline specified by the Exchanges, appropriate disciplinary action shall be initiated by the Exchange, after following due process and providing opportunity of hearing.

IX. Periodic Audit The Terms of Reference for the System Audit of Members, specified vide circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013, shall be modified to include Auditor's comment on the implementation of the aforementioned guidelines and any ongoing compliance requirements.

Prevention of incidents of Technical Glitches:

To ensure non-occurrence of technical glitches at our office, following preventive measures are being considered as advised by exchanges:

1 Capacity Planning:

i. Increasing number of investors may create an additional burden on the trading system of Members and hence, adequate capacity planning is a prerequisite for Members to provide continuity of services to their clients.

ii. Members shall do capacity planning for the 'Critical Systems' infrastructure including server capacities, network availability, bandwidth, and the serving capacity of trading applications.

iii. Capacity planning shall be done based on the rate of growth in the number of transactions observed in the past 2 years. This data should be extrapolated to predict the capacity required for the next 3 years.

iv. The capacity planning by Members should be done every year to review the available capacity, peak capacity, and new capacity required to tackle future load on the system. The purpose shall include all 'Critical Systems' operated in-house or through a Vendor/Application service provider (ASP).

v. Members shall monitor peak load in their 'Critical Systems' including the trading applications, servers, and network architecture. The Peak load shall be determined based on the highest peak load observed by the Members during a calendar quarter. The installed capacity shall be at least 1.5 times (1.5x) of the observed peak load.

vi. Members shall deploy adequate monitoring mechanisms within their networks and systems to get timely alerts on the current utilization of capacity going beyond the permissible limit of 70% of its installed capacity. In case the actual capacity utilization nears 70% of the installed capacity, immediate action shall be taken to avoid a breach of capacity.

vii. Adequate capacity planning and its review should be part of the annual system audit of the Members.

viii. Additionally, to ensure the continuity of services at the primary data center, ‘Specified Members’ shall strive to achieve full redundancy in their IT systems that are related to the ‘Critical Systems’.

2. Software testing and change management:
i. Software applications are prone to updates/changes and hence, it is imperative for the Members to ensure that all software changes that are taking place in their applications are rigorously tested before they are used in production systems. Software changes could impact the functioning of the software if adequate testing is not carried out. In view of this, Members shall adopt the following framework for carrying out software-related changes/testing in their systems.
ii. Members shall create test-driven environments for all types of software developed by them or their vendors.
iii. Members, during all relevant phases of software development and operations are required to write exhaustive unit test cases and functional test cases covering all positive & negative scenarios, regression testing, security testing, and non-functional testing including performance testing, stress testing, load testing, etc.
iv. Further, Members shall prepare and maintain a traceability matrix between functionalities and test cases for all ‘Critical Systems’.
v. A Minimum number of unit test cases required for every change made in the software should be defined in advance, based on its functionality, and ensure sufficient test coverage around instructions count, branches, and complexities. This would include base cases for the overall platform, plus specific sets of cases for each module under consideration.
vi. In addition to the above, ‘Specified Members’ shall perform software testing in ‘automated environments’. The ‘automated environments’ shall be mandatorily set up by ‘Specified Members’ before June 30, 2023.
vii. To ensure system integrity and stability, all changes to the installed system shall be planned, evaluated for risk, tested, approved, and documented. Members shall implement a change management process to avoid any risk arising due to unplanned and unauthorized changes for all its information security assets (hardware, software, network, etc.).
viii. Change management process shall be well documented and approved by the Governing Board of the Member.
ix. The Exchange has provisioned test environments and conducts periodic mocks for Members to test their systems. Members are required to participate in such environments, each time their systems have gone through changes before such changes are made live.
x. Members shall have a documented process/procedure for the timely deployment of patches for mitigating all identified vulnerabilities. The patch management process shall also be approved by the Governing Board of Members.
xi. Members shall periodically update all their assets including Servers, OS, databases, middleware, network devices, firewalls, IDS /IPS desktops, etc. with the latest applicable versions and patches.
xii. Review of Adequate Change Management and Patch Management processes should be part of the system audit of the Members. As a part of the mandated annual System Audit, the System Auditor shall also provide its comments and observations on the said processes, if any.

3. Monitoring mechanism - Applicable to ‘Specified Members’

i. Proactively and independently monitoring technical glitches shall be one of the approaches in mitigating the impact of such glitches. In this context, the ‘Specified Members’ shall build API-based Logging and Monitoring Mechanism (LAMA) to allow stock exchanges to monitor the ‘Key Parameters’ of the ‘Critical Systems’. Under this mechanism, ‘Specified Members’ shall monitor key systems & functional parameters to ensure that their trading systems function in a smooth manner. Stock exchanges will, through the API gateway, independently monitor these key parameters in real-time to gauge the health of the ‘Critical Systems’ of the ‘Specified Members’.

ii. Through the ‘LAMA’ Gateway, values of the ‘Key Parameters’ listed below should be served by the ‘Specified Members’.

Key Parameters for 'LAMA'		
Application	**System**	**Network**
1. Log monitoring	1. CPU Utilization	1. Packet Error Counts
2. Requests/Second	2. Memory Utilization	2. Bandwidth Utilization
3. Average response times	3. Disk utilization	3. DNS failures
4. Trading trend analysis-related data	4. Database replication and its Health	
5. Trading API failure counts	5. Uptime	
6. Network Latency		

iii. The ‘Specified Members’ and the Exchange will preserve the logs of the key parameters for a period of 30 days in the normal course. However, if a technical glitch takes place, the data related to the glitch shall be maintained for a period of 2 years. ‘Specified Members’ will be notified by the Stock Exchanges, for onward discussion on the implementation and applicability of ‘LAMA’ and its key parameters.

4. Business Continuity Planning (BCP) and Disaster Recovery Site (DRS):

i. ‘Specified Members’ and Members with a minimum client base of 50,000 clients across all Exchanges, are to mandatorily establish a ‘Business Continuity’/ ‘Disaster Recovery setup’.

ii. Members shall put in place a comprehensive BCP-DR policy document outlining standard operating procedures to be followed in the event of any ‘Disaster’.

iii. ‘Disaster’ may be defined as scenarios where:

a. A 45-minute disruption of any of the ‘Critical Systems’, or

b. Any additional criteria specified by the Governing Board of the Member.

iv. The DRS shall preferably be set up in different seismic zones. In case, due to any reasons like operational constraints, such a geographic separation is not possible, then the Primary Data Centre (PDC) and DRS shall be separated from each other by a distance of at least 250 kilometers to ensure that both do not get affected by the same natural disaster. The DR site shall be made accessible from the primary data center to ensure syncing of data across two sites.

v. ‘Specified Members’ shall conduct DR drills/live trading from the DR site on half yearly basis. DR drills/ live trading shall include running all operations from DRS for at least 1 full trading day.
vi. Members shall constitute responsible teams for taking decisions about shifting of operations from primary site to DR site, putting adequate resources at DR site, and setting up mechanism to make DR site operational from primary data center etc.
vii. Hardware, system software, application environment, network and security devices, and associated application environments of DRS and PDC shall have a one-to-one correspondence between them. Adequate resources shall be always made available to handle operations at PDC or DRS.
viii. The Recovery Time Objective (RTO) i.e., the maximum time taken to restore operations of ‘Critical Systems’ from DRS after the declaration of ‘Disaster’ shall be 2 Hours and, Recovery Point Objective (RPO) i.e., the maximum tolerable period for which data might be lost due to a major incident shall be 15 Minutes.
ix. Replication architecture, bandwidth, and load consideration between the DRS and PDC shall be within the stipulated RTO and the whole system shall ensure high availability, right-sizing, and no single point of failure. Any updates made at the PDC shall be reflected at DRS immediately.
x. The BCP-DR policy document shall be reviewed at least once a year to minimize incidents affecting business continuity. Additionally, an Adhoc review of the BCP-DR policy shall also be conducted in case of any major changes in ‘Critical Systems’ and if any technical glitch is encountered. The BCP-DR policy document of the Members should be approved by Governing Board of the Members.
xi. The Governing Board of the Members shall review the implementation of BCP-DR policy approved by the Governing board of the Members on a Quarterly basis. Further, Members shall conduct periodic training programs to enhance the preparedness and awareness level among its employees and outsourced staff, vendors, etc. to perform as per BCP policy.
xii. The System Auditor, while covering the BCP – DR as a part of mandated annual System Audit, shall check the preparedness of the Member to shift its operations from PDC to DRS and comment on documented results and observations on DR drills conducted by the Members.
xiii. The ‘Specified Members’ shall constitute an Incident and Response Team (IRT) / Crisis Management Team (CMT), which shall be chaired by the Managing Director (MD) of the Member or by the Chief Technology Officer (CTO), in case of non-availability of MD. IRT/CMT shall be responsible for the actual declaration of disaster, invoking the BCP and shifting of operations from PDC to DRS whenever required. Details of roles, responsibilities, and actions to be performed by employees, IRT/ CMT and support/outsourced staff in the event of any Disaster shall be defined and documented by the Members as part of BCP-DR Policy Document.
xiv. In addition to the above, ‘Specified Members’ shall obtain ISO27001 (Information Security) certification within the 2 years, from April 1, 2023. Additionally, ISO20000 (IT Service Management) and ISO22301 (Business Continuity Management System) are recommended to be adhered to. All Policies procedures and processes must be based on these international Standards.

Financial Disincentives and Penalty Structure **ANNEXURE C**

Sr. No.	Instances of technical glitches	Financial disincentives	
		Specified Members	**All other Members**
1.	**Technical Glitch continuing for more than 15 minutes:**		
	First instance	Observation Letter	Observation Letter
	Second instance	Administrative warning	Administrative warning
	Third instance onwards	For every instance Rs. 50,000/- It will progressively increase by Rs.25,000/- for subsequent instances. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance shall decide on additional disciplinary actions.	For every instance Rs. 20,000/- It will progressively increase by Rs.5,000/- for subsequent instances. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance shall decide on additional disciplinary actions.
2.	**More than 5 Technical Glitch Incidents during the financial year.** **(Incidents lasting more than 15 minutes)**	In addition to the penalty already levied as per the above provisions, no on-boarding of new clients till stock exchange analyses RCA and satisfies itself about corrective measures taken or, 15 days from glitch whichever is higher. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance	The relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance shall decide on the disciplinary actions.

		shall decide on additional disciplinary actions.	
3.	**Failure to restore operations by moving to DR site within Recovery Time Objective.**	Rs.2 lac	Rs. 20,000/-
4.	**Failure to inform Exchange about the incident/glitch within 1 hour**	Rs.50,000/-, plus Rs. 25,000/- per day till failure continues. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance shall decide on additional disciplinary actions.	Rs. 20,000/-, plus Rs. 5,000/- per day till failure continues. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance shall decide on additional disciplinary actions.
5.	**Failure to submit the preliminary incident report to the Exchange by T+1 day**		
6.	**Failure to timely submit RCA within 14 days**		
7.	**Failure to conduct DR drill/live trading from DR site as per the provisions**	Rs. 2 lac, plus Rs. 1 lac for every month during which failure continues. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance shall decide on additional disciplinary actions.	NA

Addendum to Framework to address the 'technical glitches' in Member's Electronic Trading Systems

Member's attention is drawn to the Exchange circular NSE/COMP/54876 dated December 16, 2022, on Framework to address the 'technical glitches' in Member's Electronic Trading Systems.

As per the circular, RCA reports for all technical glitch incidents greater than 45 minutes shall also be verified by an independent auditor appointed by the Member.

Trading Members are required to submit Root Cause Analysis (RCA) Report of the technical glitch to the Exchange, within 14 days from the date of the incident. Furthermore, in the case of technical glitch incidents lasting more than 45 minutes, an independent auditor's report on the RCA shall be submitted within 45 days of the incident.

M. BACKUP POLICY

All important data backup is taken on daily basis. Backup is taken to prevent loss of data in the event of equipment failure or destruction.

Backup Storage -There shall be a separate or set of storage for each backup day. The old data is kept for 7 days and after that the storage media is reused.

Monthly Backups-Every month a monthly backup shall be made using the latest backup on the USB hard disk and the same is taken to separate location by the directors.

For **K.M.Jain Stock Brokers Pvt Ltd**
Director & Compliance Officer - Anand Jain