**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*

**ADOPTED BY K M Jain Stock Brokers Pvt Ltd as on 22.12.2021**

**K.M.Jain Stock Brokers Pvt Ltd**
Policies created by: Anand Jain
Policies reviewed by: Madhulika Jain
Policies reviewed on: 11th May, 2026
Policies approved by: Board of Directors
Policies approved on: 11th May, 2026

**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:<br><br>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<br><br>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 <u>more than 15 minutes</u>:** | | |
| | **First instance** | Observation Letter | Observation Letter |
| | **Second instance** | Administrative warning | Administrative warning |
| | **Third instance onwards** | For every instance Rs. 50,000/-<br><br>It will progressively increase by Rs.25,000/- for subsequent instances.<br><br>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/-<br><br>It will progressively increase by Rs.5,000/- for subsequent instances.<br><br>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.**<br><br>**(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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.