MSE
METROPOLITAN STOCK EXCHANGE

Department: Information Technology	**Segment: All**
Circular No: MSE/IT/12759/2022	**Date: December 19, 2022**

Subject: Framework to address the 'technical glitches' in Member's Electronic Trading Systems.

To All Members,

SEBI circular SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022, on Framework to address the 'Technical Glitches' in Stock Brokers' Electronic Trading System.

Members of the Exchange, through various circulars, and guidelines, issued from time to time, have been required to put in place various measures/controls, to prevent system failures and to ensure the provision of seamless service/facilities to their clients.

In furtherance to the above, in consultation with SEBI and other Exchanges, it has been decided to issue guidelines/ Standard Operating Procedure (SOP) for handling technical glitches at the Members end as well as provide a framework for Capacity Planning, Software Testing, Change management and Business Continuity Planning (BCP)/Disaster Recovery (DR).

The guidelines, as stated in the SEBI circular SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022, have been enclosed as '**Annexure-A**' and shall be effective from **April 1, 2023**, and are applicable to all members providing '**Internet and Wireless technology-based trading facility' (IBT/STWT)** to their clients.

In specific, points 3.viii, 4.vi, 5.i, 5.ii, 5.iii, 6.v, 6.xiii, 6.xiv are only applicable to '**Specified Members**', over and above the other points as stated in '**Annexure A**'.

The top 20 Members registered with the Exchange, having the most Internet and Wireless technology-based **(IBT/STWT)** clients are classified as '**Specified Members**' for this purpose.

'**Specified Members**' shall be communicated with the additional details of the circular in due course, by the Exchange.

Members are required to take note of the same.

For and on behalf of
Metropolitan Stock Exchange of India Limited

Jibananda Bain
Chief Information Security Officer

Annexure A

1. Definition:

'Technical glitch' shall mean any malfunction in the Member's systems including malfunction in its hardware, software, networks, processes, or any products or services provided by the Member in the electronic form. The malfunction can be on account of inadequate Infrastructure/systems, cyberattacks/incidents, procedural errors, and omissions, or process failures or otherwise, in their own systems or the one outsourced from any third parties, which may lead to either stoppage, slowing down or variance in the normal functions/operations/services of systems of the Member for a contiguous period of five minutes (5 minutes) or more.

'Critical Systems' are defined as all IT systems that are related to trading applications and trading related services.

2. Reporting Requirements for Technical Glitch Incidents:

All Members shall be required to report to the Exchange any technical glitches as under:

i. All Members shall inform about the technical glitch to the stock exchanges immediately but not later than 1 hour from the time of occurrence of the glitch.
ii. Members shall submit a Preliminary Incident Report to the Exchange within T+1 day of the incident ('T' being the date of the incident). The report shall include the date and time of the incident, details of the incident, effect of the incident, and immediate action taken to rectify the problem.
iii. Members shall submit a Root Cause Analysis (RCA) Report of the technical glitch to the stock exchange, within 14 days from the date of the incident. The RCA report, for all technical glitch incidents greater than 45 minutes, shall also be verified by an independent auditor appointed by the Member.

Submission of all the above three reports shall be as per the format provided in '**Annexure B**' of this circular.

The reporting would be made to a dedicated email address **infotechglitch@nse.co.in**, which is common across the Exchanges.

Financial Disincentives and Penalties with respect to non-compliance with the provisions of the circular have been enclosed as '**Annexure C**'

3. 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 tothe'Critical Systems'.

4. 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.

5. **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.

6. **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.

Annexure: B

INTIMATION & SUBMISSION OF TECHNICAL GLITCH

	HEADERS	**DETAILS**
1. Intimation of Incident (T-day, within 1 Hour of the Incident)	1. Letter / Report Subject -	
	Name of the Member -- Member Code -	
	2. Designated Officer (Reporting Officer details)	Name: Mobile: Email ID:
	3. Date & Time of Incident	
	4. Exchanges on which Technical Glitch was encountered (NSE, BSE, MCX, NCDEX, MSEI)	
	5. Intimation to clients about the Technical Glitch. (Please attach screenshots of communications to clients)	
	6. Network Connectivity Issues / Hardware Issues / Software Issues / Human Error / Other (Please Specify (if more than one, please separate with commas))	
	7. Additional Details about the Technical Glitch, if Any.	
2. Preliminary Incident Report (T+1 day)	1. Date & Time of Incident & Incident duration (in Minutes)	
	2. Incident Description	
	3. Immediate action taken (provide brief details)	
	4. Business Impact i) Number of Clients Impacted ii) Any other impact	
	5. Were alternate trading channles available for clients (list all the alternate channels) i) Was there a spike in traffic on the alternate channels available to clients? If yes, provide details.	
	6. Was the issue caused or encountered by a third-party vendor or service provider? i) Name of the third-party vendor or service provider and a bief description of the issue. ii) Do you have a back-up vendor for the said services	
	7. Was the issue encountered on the Exchange-provided environment? If Yes, kindly provide details of initimation and communication sent to the Exchnage.	
	8. Did you move operations to the Disaster Recover (DR) site? If, Yes, what was the Recovery Time?	
3. RCA of Technical Glitch Incident (T + 14 days)	1. Date & Time of Incident & Recovery & Incident duration (in Minutes)	
	2. Incident Description & chronology of events (Please provide brief details)	
	3. Business Impact: Please provide details on the points below: i) Number of clients impacted ii) Number of client orders impacted iii) Any P&L impact iv) Any other impact on Business	
	4. Details of Client Complaints Received (Please provide details of claims of impacted clients) i) Number of Complaints Received ii) Number of Complaints Settled iii) Number of pending complaints iv) Total amount claimed by complainants	
	5. Root Cause Summary (Pl attach the detailed Report separately)	
	6. If the issue was caused or encountered by a third-party vendor or service provider, Please provide the below details: i) What services are being provided by the third-party vendor or service provider? ii) Time taken (in Minutes) by third-party vendor or service provider to resolve the issue.	
	7. Has a similar issue been encountered prior to the submission of this RCA Report?	
	8. Details of long-term preventive action (please provide all action points for long-term preventive action with the date from which they will be implemented) (please use additional sheets if necessary)	
	9. Provide a detailed Architecture Diagram of the System.	

ANNEXURE C
Financial Disincentives and Penalty Structure

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 noncompliance 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 shall decide on additional disciplinary actions.	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.
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.	Rs. 20,000/-, plus Rs. 5,000/- per day till failure continues.

5	**Failure to submit the preliminary incident report to the Exchange by T+1 day**	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.	Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of noncompliance shall decide on additional disciplinary actions.
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