

---

**Review of Framework to address the 'Technical Glitches' in Stock Brokers'  
Electronic Trading Systems**

---

This is with reference to the SEBI circular no. SEBI/HO/ 38/44/12(1)2026-MIRSD-TPD1, dated January 9, 2026, regarding Review of Framework to address the 'technical glitches' in Stock Brokers' Electronic Trading Systems. The circular is enclosed herewith for ready reference.

In view of the above mentioned SEBI circular and as advised by SEBI, Stock Exchanges have jointly framed detailed guidelines on – definition of Technical Glitch, applicability of framework, Capacity Planning, Software Testing & Change Management, Business Continuity Planning (BCP) & Disaster Recovery Site (DRS) and Monitoring Mechanism which is mentioned as **Annexure – 1**.

Further, the revised financial disincentives structure for technical glitch incidents at Stock Brokers/Trading Member's electronic trading system is mentioned as **Annexure A**. The reporting formats of preliminary incident report and Root Cause Analysis (RCA) is mentioned as **Annexure B & C** respectively.

The provisions of the circular will come into immediate effect from January 09, 2026.

Members are requested to take note of the above and ensure compliance.

For and on behalf of  
Multi Commodity Exchange of India Ltd.

Abhay Angarkar  
VP – Technology

---

Kindly contact Customer Service Team on 022 – 6649 4040 or send an email at [customersupport@mcxindia.com](mailto:customersupport@mcxindia.com) for any clarification.

**CIRCULAR**

HO/38/44/12(1)2026-MIRSD-TPD1

January 09, 2026

**To****All recognized Stock Exchanges****All Registered Stock Brokers through Recognized Stock Exchanges**

Dear Sir/ Madam,

**Sub: - Review of Framework to address the 'technical glitches' in Stock Brokers' Electronic Trading Systems'**

1. SEBI vide Circular No. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022 laid down a comprehensive framework to address the technical glitches in stock brokers' electronic trading systems. Subsequently, Stock Exchanges also issued detailed guidelines in this regard on December 16, 2022.
2. SEBI received several representations from the various stakeholders and Industry forum regarding need to review the present framework on Technical glitches. Based on the representation received and the analysis of the technical glitch data, a public consultation paper was prepared and disseminated on SEBI website to obtain views from all the stakeholders. A views/feedback obtained on a consultation paper was analysed and discussed with stakeholders.
3. The extant technical glitch framework for the stock brokers is thus modified. The modification is carried out based on the following broad principles:
  - 3.1 Ease of compliance: The eligibility criteria has been streamlined to exclude smaller size stock brokers from the technical glitch framework to reduce overall compliance of such stock brokers.
  - 3.2 Exemptions from applicability: The technical glitches which are outside the stock brokers' trading architecture, glitches that don't directly affect the

trading functionality and those which have negligible impact have been exempted from the technical glitch framework.

3.3 Simplifying the reporting requirement: Extension of time for reporting of technical glitches (*from one hour to two hours*), consideration of trading holiday's while submitting reports and streamlining the reporting requirement from reporting to all the exchanges to a single reporting platform (i.e. *Common Reporting Platform*)

3.4 Rationalised and cost effective based technology requirements: The requirements for the capacity planning, software testing and DR drill have been rationalised based on the size of the stock brokers & their technology dependency.

3.5 Rationalisation in disincentive structure: The financial disincentive structure has been rationalised considering the exemptions, type of glitches (major or minor) and the frequency of the occurrences.

4. The revised framework for Technical glitch is as under.

5. Definition of Technical Glitch:

5.1 *“Technical glitch shall mean any malfunction in the electronic system of stock broker, including malfunction in its hardware, software, networks/bandwidth, processes or products or services, directly or indirectly related to trading and risk management, occurred during trading session of stock exchange. The malfunction in the systems of stock brokers or the one outsourced from any third parties, which may lead to either stoppage, slowing down or variance in the trading and risk management functions such as log-in, order placement (including modification, cancelation, execution, confirmation, status), allocation and viewing of margin/ collateral/ funds etc., for a contiguous period of five minutes or more.”*

5.2 The above definition of technical glitches is subject to the condition that the following types of technical issues in the system of stock brokers shall not be considered as technical glitches irrespective of the time of occurrence and accordingly need not be reported to Exchanges;

- i. Technical glitches occurred due to global issues such as malfunction or technical disruption at the cloud service providers or any other global technology provider or any technical issue causing widespread disruption
- ii. Technology disruption due to technical issues at MII
- iii. Technological glitches observed while processing of new trading account (KYC process)
- iv. Technical issues at the Back-office which does not impact the trading and settlement of the clients
- v. The failure of payment gateway applications due to technical issues exist at banks or at the service provider or at payment aggregators end.
- vi. Technical issues observed in the decision support tools such as technical charts, profit and loss statements, back office reports etc.”

5.3 Exchanges have introduced financial disincentive structure for occurrence of technical glitches. In this context, financial disincentive structure shall not be applicable for the technical glitches which do not affect the stock broker's ability to provide seamless services to their clients. In case of the following types of technical glitches, the financial disincentive structure shall not be applicable:

- A technical glitch that occurred one of two modes of trading (*i.e either in the mobile-based trading application or in the web-based trading application*) while other mode of the trading is functioning in proper manner
- A technical glitch that is minor in nature or has a minor impact on the seamless operations of the stock brokers.

Stock exchanges shall issue detailed guidelines in this regard in consultation with SEBI.

6. Applicability of framework:

6.1 The framework shall be applicable to the stock brokers providing IBT/STWT trading platforms and having more than 10,000 registered clients (*excluding closed accounts*) as on 31<sup>st</sup> March of previous financial year.

6.2 Stock exchange shall issue detailed guidelines in this regard and disseminate the list of applicable stock brokers.

7. Reporting Requirements:

7.1 Stock brokers shall inform regarding the technical glitch to the stock exchanges and also to their clients within 2 hours from the time of occurrence of the glitch. Exchanges in turn shall disseminate the technical glitch incidents on their website.

7.2 Stock brokers shall inform their clients regarding the occurrence of technical glitch by disseminating information on their website and any other mode such as SMS/email/pop-up in mobile based/ web based trading application etc.

7.3 Stock brokers shall submit a Preliminary Incident Report (*as per the format prescribed by stock exchanges*) to the stock exchange within T+1 day of the incident (T being the date of the incident). However, if T+1 day falls on a trading holiday; submission may be done on next trading day.

7.4 Stock brokers shall submit a Root Cause Analysis Report (RCA) (*as per the format prescribed by stock exchanges*) of the technical glitch to stock exchange, within 14 working days from the date of the incident.

7.5 Stock brokers shall submit information/reports mentioned above, on 'Samuhik Prativedan Manch' i.e. common portal for submissions by stock brokers.

7.6 All technical glitches reported by stock brokers as well as independently monitored by stock exchanges, shall be examined by the stock exchanges for suitable actions.

8. Capacity Planning:

8.1 Increasing number of investors create additional burden on the trading system of the stock broker and hence, adequate capacity planning is prerequisite for stock brokers to provide continuity of services to their clients. Stock brokers shall do capacity planning for entire trading infrastructure i.e. server capacities, network availability, and the serving capacity of trading applications.

8.2 Stock brokers shall monitor peak load in their trading applications, servers and network architecture.

8.3 Stock exchanges shall issue detailed guidelines with regard to capacity planning, peak load, and new capacity required to tackle future load on the system of the stock brokers. The extant guidelines shall be rationalised based on the size of the stock brokers & their technology dependency.

9. Software testing and change management

9.1 Software applications are prone to updates/changes and hence, it is imperative for the stock brokers 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 resulting technical glitches in such software.

9.2 Stock exchanges shall issue detailed guidelines with regard to testing of software, traceability matrix, change management process and periodic updation of assets etc. The extant guidelines shall be rationalised based on the size of the stock brokers & their technology dependency.

10. Monitoring mechanism:

10.1 Proactively and independently monitoring technical glitches shall be one of the approaches in mitigating the impact of such glitches. In this context, Stock Exchanges have deployed API based Logging and Monitoring Mechanism (LAMA). Stock exchanges shall continue to monitor the trading systems of the stock brokers through this mechanism.

10.2 Stock exchanges shall review the applicable provisions of LAMA and issue detailed guidelines with regard to applicability, key monitoring parameters and preservation of logs etc.

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

11.1 Stock Exchanges shall review the current guidelines for the applicability of the BCP and DRS. The current guidelines shall be rationalised based on the size of the stock brokers & their technology dependency ensuring the following

- i BCP and DRS shall not be applicable to small size stock brokers.
- ii Setting up of DR site in different seismic zones
- iii Frequency of DR drill and trading from DR site
- iv Defining Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and defining the term “Disaster” for the implementation of the DR.
- v Requirement for the coverage of BCP-DR during the System Audit and ISO certification requirements.

12. Stock exchanges shall rationalise and revise the current structure of the financial disincentives considering the applicable exemption for technical glitches, type of glitches (major or minor) and the frequency of occurrences of the glitches.



13. Stock exchanges shall disseminate on their websites the instances of technical glitches occurred in the trading system of stock brokers.
14. This circular shall supersede earlier SEBI circular no SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022.
15. Stock exchanges shall build necessary systems for implementation of the provisions of this circular and issue appropriate guidelines to the stock brokers for the compliance with the provisions of this circular.
16. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act 1992 and Regulation 50 of SEBI (Stock Brokers) Regulations 2026, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.
17. This circular is available on SEBI website at [www.sebi.gov.in](http://www.sebi.gov.in) under the categories “Legal Framework” and “Circulars”.
18. This circular shall come into effect from January 09, 2026.

Yours faithfully,

**Vishal M Padole**  
**General Manager**  
**Market Intermediaries Regulation and Supervision Department**  
**Tel. No: 022 26449247**  
**Email ID: [vishalp@sebi.gov.in](mailto:vishalp@sebi.gov.in)**



**Detailed guidelines on Review of technical glitch framework for stock brokers**

**1. Definition of Technical Glitch:**

1.1 “Technical glitch shall mean any malfunction in the electronic system of stock broker, including malfunction in its hardware, software, networks/bandwidth, processes or products or services, directly or indirectly related to trading and risk management, occurred during trading session of stock exchange. The malfunction in the systems of stock brokers or the one outsourced from any third parties, which may lead to either stoppage, slowing down or variance in the trading and risk management functions such as log-in, order placement (including modification, cancelation, execution, confirmation, status), allocation and viewing of margin/ collateral/ funds etc., for a contiguous period of five minutes or more.”

1.2 The above definition of technical glitches is subject to the condition that the following types of technical issues in the system of stock brokers shall not be considered as technical glitches irrespective of the time of occurrence and accordingly need not be reported to Exchanges;

- i. Technical glitches occurred due to global issues such as malfunction or technical disruption at the cloud service providers or any other global technology provider or any technical issue causing widespread disruption
- ii. Technology disruption due to technical issues at MII
- iii. Technological glitches observed while processing of new trading account (KYC process)
- iv. Technical issues at the Back-office which does not impact the trading and settlement of the clients
- v. The failure of payment gateway applications due to technical issues exist at banks or at the service provider or at payment aggregators end.
- vi. Technical issues observed in the decision support tools such as technical charts, profit and loss statements, back office reports etc.”

## 2. Threshold for exemption from disincentive structure

The financial disincentive structure has been rationalised considering the exemptions, type of glitches (major or minor) and the frequency of the occurrences. The Financial disincentive structure is applicable for the technical glitches which continued for more than 15 minutes. The revised Financial disincentives structure with respect to non-compliance with the provisions of the technical glitch framework is enclosed as '**Annexure A**'

2.1 The disincentive structure is not applicable if the technical glitches falls under the definition of glitches, however such glitches do not affect the stock broker's ability to provide seamless services to their clients. Therefore, in case of the following types of technical glitches, the financial disincentive structure shall not be applicable:

- ❖ A technical glitch that occurred either in the mobile-based trading application or in the web-based trading application while either of them is functioning in a proper manner.
- ❖ A technical glitch that is minor in nature or has a minor impact on the seamless operations of the stock brokers.

2.2 The exemption from financial disincentive structure mentioned at para 2.1 above is subject to the following:

- a. In case of QSBs and 'specified stock brokers (*defined at para 89 below*)', unique clients affected due to technical glitch shall not be more than [*average of 1% unique clients (segment wise/exchange wise) traded in previous quarter or 5,000 unique clients (segment wise/exchange wise) whichever is lower*].
- b. In case of other stock brokers', unique clients affected due to technical glitch shall not be more than [*average of 2% unique clients (segment wise/exchange wise) traded in previous quarter or 2000 unique clients (segment wise/exchange wise) whichever is lower*].

2.3 Stock broker is required to demonstrate to the Stock Exchange based on the audit of logs' etc. that the above mentioned threshold criteria is met. Stock broker shall submit system auditor's certificate to stock Exchange in this regard.

### 3. **Applicability of the technical glitch framework:**

3.1 The framework shall be applicable to the stock brokers providing IBT/STWT trading platforms and having more than 10,000 registered clients (*excluding close accounts*) as on 31st March of previous financial year.

### 4. **Reporting requirements:**

4.1 Stock brokers shall inform the occurrence of the technical glitch to the stock exchanges and also to their clients within 2 hours from the time of occurrence of the glitch. Exchanges in turn shall disseminate the technical glitch incidents on their website.

4.2 Stock brokers shall inform their clients regarding the occurrence of technical glitch by disseminating information on their website and any other mode such as SMS/email/pop-up in mobile based/ web based trading application etc.

4.3 Stock brokers shall submit a Preliminary Incident Report (**Annexure B**) to the stock exchange within T+1 day of the incident (T being the date of the incident). However, if T+1 day falls on a trading holiday; submission may be done on next trading day.

4.4 Stock brokers shall submit a Root Cause Analysis Report (RCA) (**Annexure C**) of the technical glitch to stock exchange, within 14 working days from the date of the incident.

4.5 Stock brokers shall submit information/reports mentioned above, on 'Samuhik Prativedan Manch' i.e. common portal for submissions by stock brokers.

### 5. **Capacity planning:**

5.1 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.

5.2 Members shall do capacity planning for the 'critical systems' including server capacities, network availability, bandwidth, and the serving capacity of trading applications.

5.3 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.

5.4 The capacity planning by Members should be done periodically 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).

5.5 The periodicity of capacity planning exercise for different type of stock brokers is as follows:

- a. QSBs shall do capacity planning on quarterly basis,
- b. 'Specified stock brokers' shall do capacity planning on half yearly basis,
- c. Remaining stock brokers shall do capacity planning on yearly basis.

5.6 Members shall monitor peak load in their 'critical systems' including servers, and network architecture. The Peak load shall be determined on the basis of highest peak load observed during a calendar quarter in case of QSB, during a calendar half year in case of specified stock brokers and, during a calendar year in case of other stock brokers.

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

5.8 The installed capacity shall be at least 2 times (2x) of the observed peak load for QSBs and 1.5 times (1.5x) of the observed peak load for 'specified stock brokers' and other stock brokers.

5.9 Stock brokers shall deploy adequate monitoring mechanisms within their networks and systems to get timely alerts on current utilization of capacity going beyond permissible limit of 70% of its installed capacity.

5.10 Adequate capacity planning and its review shall be a part of the annual system audit of the Members.

5.11 To ensure the continuity of services at the primary data centre, members shall strive to achieve full redundancy in their IT systems that are related to 'critical systems'.

## **6. Software testing and change management:**

6.1 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.

6.2 Members shall create test-driven environments for all types of software developed by them or their vendors.

6.3 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.

6.4 Further, Members shall prepare and maintain a traceability matrix between functionalities and test cases for all 'critical systems'.

6.5A 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.

6.6 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.).

6.7 Change management process shall be well documented and approved by the Governing Board of the Member.

6.8 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.

6.9 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.

6.10 Members shall periodically update all their assets including Servers, OS, databases, middleware, network devices, firewalls, IDS /IPS desktops etc. with latest applicable versions and patches.

6.11 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.

## **7. Monitoring mechanism**

7.1 Proactively and independently monitoring technical glitches shall be one of the approaches in mitigating the impact of such glitches. In this context, the 'Specified stock brokers' 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 stock brokers' 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 stock brokers'.

7.1 Through the 'LAMA' Gateway, values of the 'Key Parameters' listed below should be served by the 'Specified stock brokers'.

Key Parameters for 'LAMA'		
Application	System	Network
Log monitoring	CPU Utilization	Packet Error Counts
Requests/Second	Memory Utilization	Bandwidth Utilization
Average response times	Disk utilization	
Trading trend analysis-related data	Database replication and its Health	
Trading API failure counts	Uptime	

7.2 The 'Specified stock brokers' 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 logs and data related to the glitch shall be maintained for a period of 2 years.

## **8 Business Continuity Planning (BCP) and Disaster Recovery Site (DRS):**

- 8.1 Members with a minimum client base of 50,000 clients across all Exchanges, are to mandatorily establish a 'Business Continuity'/ 'Disaster Recovery setup'.
- 8.2 Members shall put in place a comprehensive BCP-DR policy document outlining standard operating procedures to be followed in the event of any disaster.
- 8.3 'Disaster' may be defined as scenarios where:
- A 45-minute disruption of any of the 'critical systems', or
  - Any additional criteria specified by the Governing Board of the Member.
- 8.4 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 kilometres to ensure that both of them do not get affected by the same natural disaster. The DR site shall be made accessible from primary data centre to ensure syncing of data across two sites.



- 8.5 '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.
- 8.6 In case if any new member falls under the purview of Technical glitch framework the DR drills/ live trading for such members shall include running operations with 30% clients from DRS for at least 1 full trading day during first quarter and with 60% clients from DRS for at least 1 full trading day during second quarter and with 100% clients from DRS for at least 1 full trading day from subsequent quarter onwards.
- 8.7 Stock brokers, 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 centre etc.
- 8.8 Hardware, system software, application environment, network and security devices and associated application environments of DRS and PDC shall have one-to-one correspondence between them. Adequate resources shall be made available at all times to handle operations at PDC or DRS.
- 8.9 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.
- 8.10 Replication architecture, bandwidth and load consideration between the DRS and PDC shall be within 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.
- 8.11 The BCP-DR policy document shall be reviewed at least once in 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.

- 8.13 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.
- 8.14 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.
- 8.15 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.
- 8.16 ‘Specified Members’ and QSBs shall obtain ISO27001 (Information Security) certification within the 2 years, from applicability of the framework. 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.
- 9 Specified stock brokers’: The top 20 stock brokers registered with the Exchange, having the most Internet and Wireless technology-based (IBT/STWT) clients are classified as ‘Specified stock brokers’ for this purpose. The list of ‘specified stock brokers’ will be published at the beginning of every financial year on the website of the stock exchange.
- 10 Members shall not consider the institutional clients for determining applicability of technical glitch framework.

**Annexure - A**

**Financial disincentive and penalty structure for technical glitch incidents at stock brokers' electronic trading system:**

Sr. No.	Instances of technical glitches	Financial disincentives	
		Specified stock brokers	All other applicable stock brokers
A) Technical Glitch continuing for <u>more than 15 minutes</u> during financial year:			
i	6 <sup>th</sup> glitch incident onwards	<p>For every instance Rs. 25,000/-</p> <p>It will progressively increase by Rs.25,000/- for subsequent instances.</p> <p>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.</p>	<p>For every instance Rs. 10,000/-</p> <p>It will progressively increase by Rs.5,000/- for subsequent instances.</p> <p>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.</p>
ii	From 7 <sup>th</sup> glitch incident to 10 <sup>th</sup> glitch incident occurred during financial year: The progressive penal provision will continue.		
iii	11 <sup>th</sup> incident onwards	<p>Progressive monetary penalty shall be applicable as per the above provisions.</p> <p>In addition to the penalty already levied as per the above provisions, on-boarding of new clients (exchange wise /segment wise depending on nature of glitches) shall be stopped till stock exchange analyses RCA and satisfies itself about corrective measures taken or, 15 days from glitch whichever is higher.</p> <p>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.</p>	<p>Progressive monetary penalty shall be applicable as per the above provisions.</p> <p>In addition to the monetary penalty applicable as per the above provisions, 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.</p>

<b>B) Other Penalties (in cases of technical glitches occurred)</b>			
i	Failure to report technical glitch incident to Exchange	Rs.5 lac	Rs.1 lac
ii	Failure to submit the preliminary incident report to the Exchange by T+1 day (However, if T+1 day falls on a trading holiday; submission may be done on next trading day)	Rs. 50,000/-, plus Rs. 25,000/- per day till failure continues subject to maximum of Rs.5 lac.	Rs. 20,000/-, plus Rs. 5,000/- per day till failure continues subject to maximum of Rs.1,00,000/-.
iii	Failure to submit RCA within 14 working days	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 non-compliance shall decide on additional disciplinary actions.
iv	Failure to set up DR site as per the provisions	Rs.2 lac	Rs. 20,000/-
v	Failure to restore operations by moving to DR site within Recovery Time Objective.	Rs.1 lac	Rs. 20,000/-
vi	Failure to conduct DR drill/live trading from DR site as per the provisions	Rs. 1 lac, plus Rs. 50,000/- for every month during which failure continues subject to maximum of Rs.5 lac per instance.  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

INTIMATION & SUBMISSION OF TECHNICAL GLITCH		
	HEADERS	DETAILS
<b>1. Intimation of Incident</b>  (T-day, within 2 Hour of the Incident )	<b>1. Letter / Report Subject -</b>	
	<b>Name of the Member --</b>	
	<b>Member Code -</b>	
	<b>2. Designated Officer (Reporting Officer details)</b>	<b>Name:</b>
		<b>Mobile:</b>
		<b>Email ID:</b>
	<b>3. Date &amp; Time of Incident</b>	
	<b>4. Exchanges on which Technical Glitch was encountered (NSE, BSE, MCX, NCDEX, MSEI)</b>	
<b>5. Intimation to clients about the Technical Glitch. (Please attach screenshots of communications to clients)</b>		
<b>6. Additional Details about the Technical Glitch, if Any.</b>		
<b>2. Preliminary Incident Report (T+1 day)</b>	<b>1. Date &amp; Time of Incident &amp; Incident duration (in Minutes)</b>	
	<b>2. Incident Description</b>	
	<b>3. Immediate action taken (provide brief details)</b>	
	<b>4. Business Impact</b> i) Number of Clients Impacted ii) Any other impact	
	<b>5. Were alternate trading channels available for clients (list all the alternate channels)</b> i) Was there a spike in traffic on the alternate channels available to clients? If yes, provide details.	
	<b>6. Was the issue caused or encountered by a third-party vendor or service provider?</b> i) Name of the third-party vendor or service provider and a brief description of the issue. ii) Do you have a back-up vendor for the said services	
<b>7. Was the issue encountered on the Exchange-provided environment? If Yes, kindly provide details of intimation and communication sent to the Exchange.</b>		

	<b>8. Did you move operations to the Disaster Recover (DR) site? If, Yes, what was the Recovery Time?</b>	
	<b>9. Network Connectivity Issues / Hardware Issues / Software Issues / Human Error / Other (Please Specify (if more than one, please separate with commas))</b>	

## Annexure - C

<b>Root Cause Analysis report (RCA)</b> (on the letterhead of stock broker)	
<b>1. Name of the Member</b>  Member Code:	
<b>2. Reporting Officer details</b>	
Name:  Designation:  E-mail:  Mobile:	
<b>3. Date and time of technical glitch incident</b> Date of incident Time of Incident	
<b>4. Date and Time of recovery</b> Date of recovery Time of Recovery Duration of the Incident	
<b>5. Incident Description &amp; chronology of events</b> (please use additional sheets if required)	
<b>6. Category of incident</b> (hardware, software application, server, network, bandwidth, vendor related, other-please specify)	
<b>7. Business Impact:</b> Number and percentage of clients affected (duly certified by Auditor) No. of complaints received No. of complaints resolved till RCA date Amount of claim made by complainant Amount of claim paid to complainant	
<b>8. Immediate action taken</b> (please give full details. Use additional sheets if required)	
<b>9. Root Cause Summary</b> (PI attach the detailed Report separately)	
<b>10. Action taken to prevent such incident in future</b>	
<b>Name and Signature of Compliance Officer/CTO</b>  <b>Date:</b>	