National Stock Exchange of India

Circular

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

To All Members,

Sub: Guidelines on Technical Glitches to prevent business disruptions

Members of the Exchange, through various circulars, guidelines, issued from time to time, have been required to put in place various measures / controls, to prevent system failures and to ensure 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 Members end as well as provide a framework for Business Continuity Planning (BCP)/Disaster Recovery (DR). The said guidelines have been enclosed as **Annexure-A** and shall be effective from in accordance with para VII.

All Members are advised to take note of the above and comply.

For and on behalf of
National Stock Exchange of India Limited

Srijith Menon
Associate Vice President
Membership Compliance Department

Encl.: Annexure-A- Guidelines for handling technical glitches

National Stock Exchange of India

Circular

Annexure-A

Guidelines for prevention of Business Disruption due to technical glitches & Standard Operating Procedures (SOP) to be adopted upon incident of Technical Glitches.

I. Objective

The objective of this guideline is to outline the technology infrastructure and system requirements that 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 Members, 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 Member's systems including malfunction in its hardware or software or any products/services provided by the Member, 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 the Member, 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.

III. Preventive Measures

a) Members 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, all Members 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, Members are also advised to 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.

2. Member should implement and deploy suitable monitoring tools to monitor the data traffic within the Member's organization network and to & from the organization network.

ii. Backup and Recovery

1. The response and recovery plan of the Members should have plans for the timely restoration of systems affected by incidents of technical glitch.
2. Member 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 Members in case of any technical glitches, so that interest of investors and market at large is not adversely impacted, all Members **with a client base of more than 50,000 unique registered clients across all Exchanges** shall be required to mandatorily establish Business Continuity/DR set up to ensure that there is well defined continuity plan in case of such Business Disruptions.

1. The Members 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

plan, members are advised to 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. Member 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.

V. Reporting Requirements

Members shall be required to report to the Exchange any technical glitches, resulting in Business Disruption. Members shall report the same to the Exchange as under:

1. Members 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.** Members 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.

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.

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 months from the date of this circular.

		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. <u>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</u>

1. <u>Delay in Reporting</u>

   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. <u>Repeat Violation</u>

   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.

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.

_____End of Document_____

National Stock Exchange of India

Circular

Exhibit-I of Annexure-A

Incident Reporting Form/ RCA	
1. Letter / Report Subject -	
Name of the Member – Member Code -	
2. Designated Officer (Reporting Officer details)	
Name:	E-mail: Mobile:
3. Date & Time of Incident & Incident duration	
4. Incident Description & chronology of events (please use additional sheets)	Brief information on the incident observed
5. Business Impact	
6. Immediate action taken (please give full details) (Please use additional sheets if necessary)	
7. Date & Time of Recovery	
8. Root Cause Summary (Pl attach the detailed Report separately)	
9. Back up measures available	
10. Details of long-term action (please give full details) (please use additional sheets if necessary)	

Note: In case of technical disruption due to Network issues, Architecture Diagram also needs to be annexed.