INTEGRATED MASTER SECURITIES PRIVATE LIMITED

Policy on Technical Glitch I Standard Operating Procedure (SOP)

as per NSE Circular No. 10/2021 dated 15th Dec 2021

(Download Ref No. NSE/COMP/50610)

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 SEBPL, 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 SEBPL'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 SEBPL, 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) The 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 us for connectivity, enabling them to create network resilience, which the member have been advised to deploy to ensure continuity of their business operations. The members are required to ensure due compliance to the same.

c) Further, we 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, the member will also 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 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) Le., 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 will also be informed to the clients by the SEBPL.

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. SEBPL has a well-documented BCP/ DR policy and plan which will cover the following:

a. Identification of all critical operations of the SEBPL and also include the process of informing clients in case of any disruptions. While putting in place the BCP/DR plan, SEBPL is 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 D R Site upon declaration of 'Disaster'.

2. SEBPL has 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 (PDq 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. SEBPL has 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.

S. 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.

However, S E B P L do not fall in the above category, hence we are not required to have a Business Continuity/DR plan under the existing regulatory provisions.

V. Reporting Requirements

SEBPL 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. SEBPL 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 is 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, we also additionally follow the SOP for handling Cyber Security incidents issued vide NSE circular ref. no. NSE/INSP/48163 dated May 03,2021.

The above shall be monitored and implemented as defined below:

1. Reporting of incident to Exchanges; immediately
2. Internal Policy for Technical Glitch 31st March 2022
3. Preventive Recovery (Para III (a) & III (b) -System Control, Network Integrity, Backup & Recovery) by 31st March 2023