**Technical glitch Policy**

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

1. **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 Betala Stock Broking Limited, 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

1. **Definition**
2. “**Technical Glitch**” shall mean any malfunction of the Betala Stock Broking Limited'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.
3. "**Business Disruption**" shall mean either stoppage or variance in the normal functions /operations of systems of the Betala Stock Broking Limited, 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 continuousperiod of more than 15 minutes in any segment of the Exchange.
4. **Preventive Measures**
5. The member should have robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating tosecurities market and provide seamless service to their clients.
6. 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 members have been advised to deploy to ensure continuity of their business operations. The members are required to ensure due compliance tothe same.
7. 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/34120L3 dated November06, 2013, and SEBI/HO/MIRSD /CIR/PB/20L8/L47 dated Dec 03, 2018, respectively and any other circulars/regulations & guidelines issued by SEBI/Exchange in this regard from timeto time.
8. Additionally, the member will also ensure the following:
   1. System Controls & Network integrity
   2. Backup and Recovery
9. **Business Continuity Plan(BCP)/ Disaster recovery (DR)**

ln order to ensure that there is continuity of business and stability in operations ofMembers in case of any technical glitches, so that interest of investors and market atlarge is not adversely impacted, all Members with a client base of more than 50,000unique registered clients across all Exchanges shall be required to mandatorilyestablish Business Continuity/DR set up to ensure that there is well definedcontinuity plan in case of such Business Disruptions.

1. Betala Stock Broking Limited has a well-documented BCP/ DR policy and plan which will cover thefollowing:

* + Identification of all critical operations of the Betala Stock Broking Limited and also include the process of informing clients in case of anydisruptions. While putting in place the B€P/DR plan, Betala Stock Broking Limited is advised to sufficiently review all potential risks along with its impact onthe business.
  + Declaration of incident as a "Disaster" viz. timelines etc. and restoration ofoperations from DR Site upon declaration of 'Disaster'.

2. Betala Stock Broking Limited has distinct primary and disaster recovery sites (DRS) for technologyinfrastructure, workspace for people and operational processes. The DRS should beset up sufficiently away (not less than 250 km), from Primary Data Centre (PDC) toensure that both DRS and PDC are not affected by the same disasters.

3. The declaration of disaster shall be reported in the preliminary report submittedto the Exchange, as specified on section V below.

4. Betala Stock Broking Limited has alternate means of communication including channel for communicationfor communicating with the clients in case of any disruption. Such communicationshould be completed within 30 minutes from the time of disruption.

5. Adequate resources (with appropriate training and experience) should be availableat the DR Site to handle all operations during disasters.

6. DR drills should be conducted by the Member on a periodic basis not exceedinghalf yearly basis.

However, Betala Stock Broking Limited do not fall in the above category, hence we are not required to have aBusiness Continuity/DR plan under the existing regulatory provisions.

1. **Reporting**

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

1. RRS should intimate the Exchange about the incident within 2 hours from the startof the glitch.

2. A preliminary incident report shall be submitted to the Exchange within T+1 day ofthe incident (T being the date of the incident). The report shall include the date andtime of the incident, the details of the incident, effect of the incident and theimmediate action ta ken.

3. Root Cause Analysis (RCA) of the issue in the format as notified by the Exchange, to besubmitted within 21 working days. The RCA must include details of the incident, timeof occurrence and recovery, impact, summary as well as a detailed analysis of thecause of incident, immediate action taken and the long-term plan of action.

4. For the purpose of the aforementioned reporting, a common dedicated email ld,across all Exchanges, is being provided: infotechglitch@nse.co.in. Members shall make the above reporting on the said email lD only. The above reporting requirements are applicable to all Members providing internetand wireless technology-based trading facility to their clients.

5. Not withstanding the above, in case of technical glitches caused by a cyber securityincident, we also additionally follow the SOP for handling Cyber Security incidents issued vide NSE circular ref.no.NSE/INSP/48163 dated May 03, 2021.

**Version Number: 1.0.0**

Effective Date: **04/01/2025**

Prepared By: **CA VIRENDRA TAPADIYA, VRDK & CO.**

Approved By: **DINESH BABULAL JAIN, DIRECTOR OF COMPANY**