

**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 9 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'.

6.5 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.

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. A 45-minute disruption of any of the 'critical systems', or
  - b. 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.