V MATHRAN & CO PRIVATE LIMITED
204 VAISHNO CHAMBERS, 6 BRABOURNE ROAD, KOLKATA 700 001
033 4602 2696 info@vmathran.com www.vmathran.com
CIN: U67120WB1997PTC086082 GSTIN: 19AABCV6314L2Z0 SEBI Regn No: INZ000200831 & IN-DP-850-2026 MEMBER: NSE, BSE, NSDL

POLICY ON TECHNICAL GLITCH

Author:	Director
Owner:	Pratik Mathran
Organization:	V MATRHRAN & CO PRIVATE LIMITED
Version No:	1.0
Date:	**01-07-2026**

Document Control

Document Title : **Technical Glitch Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	01-07-2026	Director	NA

Approvals

Name	Title	Date of Approval	Version No
Pratik Mathran	Technical Glitch Policy	01-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

TABLE OF CONTENT

1.0 TECHNICAL GLITCH

1.1 OVERVIEW

A Technical Glitch is any observable occurrence in a system or network.

Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

This guide addresses only adverse events that are computer security related, not those caused by natural disasters, power failures, etc.

1.2 PURPOSE

The Purpose of this policy is to resolve any Technical Glitch as per the *NSE Circular Ref. No: 108/2021* read with other relevant circulars of the respective exchanges

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, 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.

1.3 SCOPE

This policy applies to:

- All staff (permanent & on contractual basis) and non-employees / stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of V Mathran & Co Private Limited and other individuals, entities or organizations that have access to and use V Mathran & Co Private Limited's information systems environment.
- V Mathran & Co Private Limited staff, who are responsible for administering and maintaining V Mathran & Co Private Limited 's IT infrastructure.

1.4 DEFINATION

Incident	An incident is an unplanned interruption or quality reduction of an IT service due to operation failure or technical glitch.
Problem	A problem is a cause, or potential cause, of one or more incidents.
Technical Glitch	Technical Glitch shall mean any malfunction of the systems including malfunction in hardware or software or any products/services provided, whether on account of any inadequacy or non-availability of infrastructure/network/ other systems or otherwise, which may lead to business disruption.
Business Disruption	Business Disruption shall mean either stoppage or variance in the normal functions /operations of systems V Mathran & Co Private Limited, due to a technical glitch, for a continuous period of more than 15 minutes
Business Continuity	Strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an accepted predefined level.
Disaster Recovery	Disaster recovery involves a set of procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

2.0 PREVENTIVE MEASURES

- V Mathran & Co Private Limited shall put in place 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. V Mathran & Co Private Limited shall deploy resiliency/redundancy measures to ensure continuity of their business operations as per guidelines issues by SEBI from time to time. V Mathran & Co Private Limited also adopt the various redundancy options provided by Exchange. However, V Mathran & Co Private Limited shall ensure due compliance while deploying the resiliency/redundancy measures.

- V Mathran & Co Private Limited shall comply with the system requirements prescribed under the PMS System Audit Framework as well as the framework for Cyber Security & Cyber Resilience prescribed by SEBI vide its Circular CIR/MRD/DMS/34/2013 and SEBI/HO/MIRSD/CIR/PB/2018/147 respectively and any other circulars/regulations & guidelines issued by SEBI/Exchange in this regard from time to time.
- V Mathran & Co Private Limited shall maintain enough capacity links to perform BAU operation including, Trading applications, BackOffice, customer support operations& connectivity to all exchange terminals with sufficient level of redundancy. Trading applications is primary working on Primary network if any disruption happens then the maximum time taken to restore and Recovery Time Objective (RTO) is 10 sec to 15 sec it switches automatically to Secondary network
- There shall be monitoring tools to monitor the data traffic within the organization network and from the organization network.
- The response and recovery plan of V Mathran & Co Private Limited shall have plans for the timely restoration of systems affected by incidents of technical glitch. V Mathran & Co Private Limited should based in their internal policy, define the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The same shall be informed to the clients by the V Mathran & Co Private Limited.

3.0 INCIDENT INFORMATION

3.1 INCIDENT INFORMATION

- If the disruption continues for more than 15 minutes, it shall be announced as an incident
- The CTO shall declare the incident
- Post declaring the incident, BCP & DR to be invoked as per BCP / DR plan
- All client communication should be completed within 30 minutes from the time of disruption. Technical glitches, resulting in business disruption needs to be reported to the exchange over common email ID: infotechglitch@nse.co.in
- V Mathran & Co Private Limited shall intimate the Exchange about the incident within 2 hours from the start of the glitch.
- 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.
- Root Cause Analysis (RCA) of the issue in the format as enclosed in Incident Management Procedure, 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.
- All incidents will be reported to Compliance, Risk Management committee and IT Steering committee.
- All communications with the media, other broadcasting channels and agencies shall be directed through the Communications team, in consultation with the CISO and CTO.
- All communications regarding business disruption with clients shall be done by the Customer Support Team the response can be vetted through Compliance/Business/Corporate Communication team & Risk team. There shall be an alternate means of communication including channel for communication for communicating with the clients in case of any Patch Scheduling & Prioritization

4.0 INCIDENT ESCALATION MATRIX

4.1 INCIDENT ESCALATION MATRIX

Refer incident management procedure for escalation matrix for incident without business disruption.

Following is the escalation matrix for technical glitch:

Level of Escalation	Escalation to:	Resolution Timelines
First Level	Crisis Management	Not resolved within 3 to 5 mins
Second Level	CRO-Chief Risk Officer/ BISO-Business Information Security Officer	Not resolved within 5 to 10mins
Third Level	CTO - Chief Technology officer / CISO – Chief Information Security Officer	Services are not up within 10 minutes

4.1.1 ROLES AND RESPONSIBILITIES

Crisis Management team, post resolution of crisis, shall update the Crisis Response Plan based on the Learning's. Business Information Security (BISO) along with the Chief Risk Officer (CRO) & Chief Technology Officer (CTO) shall review the Crisis Response Plan at least once in year and 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 plan shall be tested.

- System Audit:
  The infrastructure specified herein above shall be subject to System Audit.

- MIS
  A quarterly MIS shall be put up to the Board on incident reported, the corrective action taken and the future plan of actions including delay in deployment of corrective measures.

- Annual Review:
  This policy to be reviewed on Annual Basis

5.0 INCIDENT RESPONSE FORM

All the incidents occurred will be maintained in the Incident response form given below:

Incident Reporting Form/RCA	
1. Letter/ Report Subject -	Name of the Member- Member Code -
2. Designated Officer (Reporting Officer details)	Name: Email: 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	

By order of the Board of Directors

V Mathran & Co Private Limited