“R.B.JAJU SECURITIES INDIA PVT. LTD.”

Technical Glitches to prevent Business disruptions Policy & Procedures

Contents

1. Purpose 4
2. Scope 4
3. Acronyms/Definitions 4
4. Crisis Management Team 5
5. Designated Officer 5
6. Technology Committee 6
7. Critical Operations and Departments 6
8. Roles and responsibilities 7
   a) Every Department Head 7
   b) TechnologyTeam 7
9. Primary SitePreventiveMeasures: 7
10. RTO -RecoveryTimeObjective. 9
11. RPO -RecoveryPointObjective. 9
12. Incident Reporting, Escalation Matrix for declaring the incident a“Disaster” 11
13. Exchange Reporting Requirements 12
14. Frequency of monitoring & implementation 12

1. Purpose

This policy is to outline the technology infrastructure and system requirements have put in place to prevent any incident of business disruption resulting from technical glitches by that **R.B.JAJU SECURITIES INDIA PVT.LTD**.

2. Scope

This policy and procedure are defined to prescribe the Standard Operating Procedures (SOP)for reporting of technical glitches by Members, handling business disruption, management of such business disruption.

3. Acronyms/Definitions

Common terms and acronyms that may be used this document.

M.D. (Managing Director) / CEO (Chief Executive Officer) - The M.D. or CEO is responsible for the overall privacy and security practices of the company.

CTO– The Chief Technology Officer/ Head of IT

DO–Designated Officer

CMT –Crisis Management Team

TC– Technology Committee

Encryption–The process of transforming information, using an algorithm, to make it unreadable to any one other Than those who have as pacific 'need to know.'

External Media–i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes, etc.

SOW-Statement of Work -An agreement between two or more parties that detail the working relationship between the parties and list a body of work to be completed.

User-Any person authorized to access an information resource.

Technical Glitch - any malfunction of the systems including malfunction in its hardware or software or any products/services provided by **R.B.JAJU SECURITIES INDIA PVT. LTD**, whether on account of any inadequacy or non-availability of infrastructure/ network/other systems or otherwise, which may lead to business disruption.

Business Disruption - Means either stoppage or variance in the normal functions /operations of systems 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.

RTO - Recovery Time Objective. It is the maximum time taken to restore the operations.

RPO - Recovery Point Objective. It is the maximum tolerable period for which data might be lost, for each of their business processes/services.

BCP - Business Continuity Planning

DR - Disaster Recovery (DR).

4. Crisis Management Team

Crisis Management Team will involve senior officials or management personnel of the members including the MD/CEO and heads of business, CIO/CTO, CISO, etc. as applicable in the **R.B.JAJU SECURITIES INDIA PVT. LTD**. 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.

All members identified within this policy are assigned to their positions by the Board of Directors. The term of each member assigned is at the discretion of the Board of Directors.

The current members of the Crisis Management Team are:
SRIKANT JAJU

(The above List is prepared basis of the multiple departments. Can be reduced to limited person)

The Crisis Management Team will meet **Half Yearly** to discuss the new initiatives, issues and to review concerns that arose during the year.

The CMT is responsible for maintaining a logoff concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the half yearly meetings.

5. Designated Officer

Designated Officer will The Designated officer will be responsible for ensuring compliance to the reporting requirements. Details of the current Designated Officer as approved by the board of directors on **"R.B.JAJU SECURITIES INDIA PVT. LTD"**:

Name: SRIKANT JAJU
Contact: 9849040888
Email Id: rbjaju93@gmail.com

6. Technology Committee

R.B.JAJU SECURITIES INDIA PVT.LTD. Has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within **R.B.JAJU SECURITIES INDIA PVT. LTD.** and act as the first line of defense in enhancing the appropriate security posture. This policy shall be reviewed annually or as a when required by the "Technology Committee".

The name, Roles and responsibility of the Technology Committee is defined in the Cyber Security & Cyber Resilience Policy.

7. Critical Operations and Departments

List of Key Departments, Business owner and technology Owner

Sr	Department	Key Application	Business Owner Name	Application Owner

8. Roles and responsibilities:

a) Every Department Head:

- List down the processes and the activities that are performed as a part of the operations carried out by them
- Define the critical data and the infrastructure needed to continue the operation from DR Site.
- Define the Process of how these processes and functions will be carried out from the disaster site
- DefinetheRolesandresponsibilitiesoftheteammemberresponsibleforcarryingoutthisactivity.
- Define the time lines to restore the services from the DR Site.
- Define the matrix on who will coordinate with the Internal IT team
- Define the matrix on who will coordinate with the vendors before and after starting the operations from DR site where necessary.
- Define who will handle the customer queries before and after starting the operations from DR site.

b) Technology Team:

- List down the critical data and the infrastructure needed to continue the operation from DR Site.
- Define the Process of how to start the infrastructure at the DR Site.
- Define the matrix on who will coordinate with the internal departments.
- Define the matrix on who will coordinate with the vendors before and after starting the operations from DR site where necessary.
- Define the Roles and responsibilities of the team member responsible for carrying out this activity from DR.
- Define the application wise time line store the services from the DR Site.

9. Primary Site Preventive Measures:

System Controls & Network Integrity

A sufficient level of redundancy should be deployed and available at the primary site for all critical systems including network and data center infrastructure.

Server Level Redundancy

R.B.JAJU SECURITIES INDIA PVT.LTD. should provision adequate redundancy at the server level for all the trading servers and other servers supporting the trading applications. In case of any hard ware failure of the primary server, the backup server from the same site can be powered on.

Network Level Redundancy

Firewall:

R.B.JAJU SECURITIES INDIA PVT.LTD. should provision adequate redundancy at the Firewall level in Active-Active Mode. In case of any hardware failure of the primary Firewall, the secondary firewall will take over the load with no disruption in the services.

Monitoring Tools:

R.B.JAJU SECURITIES INDIA PVT.LTD. should provision to deploy suitable monitoring tools to monitor the data traffic within the Member's Organization network and to & from the organization network.

Exchange link:

R.B.JAJU SECURITIES INDIA PVT.LTD. should provide adequate redundancy at the Exchange Links by taking links from 2 different service providers. In case of any failure of the primary Link the load is switched over to the secondary Link seamlessly.

Internet Link:

R.B.JAJU SECURITIES INDIA PVT.LTD. should provision adequate redundancy at the Internet Links by taking links from 2 different service providers. In case of any failure of the primary Link the load is switched over to the secondary Link seamlessly.

Phone Line:

R.B.JAJU SECURITIES INDIA PVT.LTD. should provision adequate redundancy at the Phone Line level by taking links from2 different service providers. Both the Connections are in Active-Active mode hence the caller can call on any of the numbers.

Backups:

R.B.JAJU SECURITIES INDIA PVT.LTD. should provision adequate Backup plans basis on the business requirements.

- Daily Backups-Full backups should be performed on Monday, Tuesday, Wednesday, Thursday, and Friday night. In case of any maintenance activity on Friday night then backups will be taken on the next day.
- Yearly Backups–Every year a yearly backup tape should be made reusing the oldest backup tape or tape set from the tape sets.
- On Demand Backups-A backup should be taken before any major business release. The retention period for these Backups is defined by the user requesting the backup.

Data Content

Data to be backed up include the following information:

- System logs
- Application event logs
- Client activity logs
- Trade logs
- Margin logs

- Audit logs
- Client data

10. RTO - Recovery Time Objective.

RTO (the Recovery Time Objective),is a metric that defines the time to recover your IT infrastructure and services following a disaster to ensure business continuity.

For instance, if you set your RTO as 2 hours, then you should be able to continue normal business operations within this timeframe in case of any disaster. If during real-life disaster recovery, you go over the given time-frame, you should either reconsider the RTO calculations or update your disaster recovery plan and procedures. To calculate RTO, consider these factors:

- The cost per hour of outage.
- The importance and priority of individual systems.
- Steps required recovering from a disaster (including individual components and processes).
- Available budget and resources.

11. RPO-Recovery Point Objective.

Recovery Point Objective is a measure of the maximum tolerable amount of data that the business can afford toloseduringadisaster.ItalsohelpsustomeasurehowlongitcantakebetweenthelastdatabackupandadisasterwithoutseriouslydamagingyourbusinessRPOisusefulfordeterminghowoftentoperformdatabackups.

(For example, if we back up your data once a day at midnight and there is a disaster at 8 AM. In this case, we will lose 8 hours of data. If our RPO is 24 hours or more, we are in good shape. But if our RPO is four hours then we are not).

The RPO has yet another layer of depth if we are considering live production datasets. Let’s imagine that our production database is down. We have the RPO of four hours; hence we can afford to lose four hours' worth of data. If our backups are done once every two hours, we have to recover the data in two hours, rather than four. Why? Because each hour of down time we actually lose data that would normally be inserted, modified, or deleted from your production data base.

Here are the factors for determining your RPO:

- Themaximumtolerableamountofdatalossthatyourorganizationcansustain.
- The cost of lost data.
- Available budget and resources.

12. Incident Reporting, Escalation Matrix for declaring the incident a “Disaster”

- Technology team will discuss the incident with the Crisis Management Team within 15minutes of the incident. The Mode of communication can be Phone, Email or Verbal.
- CrisisManagementTeamwillmakethefinaldecisionandinformtheDesignatedOfficeraswellasthecompliance officer. The Mode of communication can be Phone or Email.
- The

Designatedofficerwillinformthecomplianceteamaswellasalltheheadsresponsibleforthebusinesscontinuity and DR operations. The Mode of communication can be Email.

- TheComplianceteamwillberesponsiblefortheintimationoftheincidenttotheexchanges.TheModeofcommunicationwill is Email.
- Compliance team indirection of the designated officer will complete the exchange formalities.
- Designated Officer will ensure the adherence of the compliance.

13. Exchange Reporting Requirements

- Members should intimate the Exchange about the incidentwithin2hoursfromthe 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 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.
- Aforementionedreportingshouldbedoneoninfotechglitch@nse.co.in

14. Frequency of monitoring & implementation

The aforementioned requirements shall be implemented as per the below timelines:

S. No.	Requirements	Time line 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- Within12 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 persecution IV.
2	Reporting of incident to Exchanges	Immediate basis
3	Internal Policy for Technical Glitch	
4	Preventive Recovery (Para III (a) &III(b) –System Control, Network Integrity, Backup & Recovery)	

Prepared By: SRIKANT JAJU
Reviewed By: SRIGOPAL JAJU
Date:
Place: HYDERABAD

************End of Document************