K.M.JAIN STOCK BROKERS PVT LTD-STOCK BROKER

CYBER SECURITY POLICIES
AND
RELATED WRITE-UPS

Policy created by : Anand Jain

Policy reviewed by : Madhulika Jain

Policy reviewed on : 31st July 2023

Policy approved by : Board of Directors

Policy approved on : 31st July 2023

FOR NSE, BSE, MCX-SX & CDSL
POLICIES & PROCEDURES ADOPTED FOR CYBER SECURITY AND DISASTER RECOVERY MANAGEMENT

Table of Contents

1. BCP and Backup policy 3
2. Before Disaster procedure 5
3. After Disaster Procedure 6
4. Password Policy 7
5. IT Access control Policy - Version Document 8
6. Organizational Chart 9
7.

1 Business Continuity Plan (BCP)

What is business continuity?

In an IT context, business continuity is the capability of your enterprise to stay online and deliver products and services during disruptive events, such as natural disasters, cyber-attacks and communication failures.

The core of this concept is the business continuity plan — a defined strategy that includes every facet of organization and details procedures for maintaining business availability.

2 BCP- business continuity plan

Business continuity management starts with planning how to maintain critical functions running (e.g., IT, sales and support) during and after a disruption.Our business continuity plan (BCP) comprises of the following elements:

2.1. Threat Analysis

The identification of potential disruptions, along with potential damage they can cause to affected resources. Examples include:

THREAT	POTENTIAL IMPACT
Power outage	Inability to access servers
Natural disasters	Critical infrastructure damage
Illness & Pandemics	Widespread employee absence
Cyber attack	Data Theft and network downtime
Vendor error	Inability to execute integrated business functions

2.2 Role assignment

Every organization needs a well-defined chain of command and substitute plan to deal with absence of staff in a crisis scenario. Employees must be cross-trained on their responsibilities so as to be able to fill in for one another.

Internal departments (e.g., marketing, IT, human resources) should be broken down into teams based on their skills and responsibilities. Team leaders can then assign roles and duties to individuals according to your organization's threat analysis.

2.3. Communications

A communications strategy details how information is disseminated immediately following and during a disruptive event, as well as after it has been resolved. Our strategy includes:

Methods of communication (e.g., phone, email, text messages)

Established points of contact (e.g., managers, team leaders, human resources) responsible for communicating with employees

Means of contacting employee family members, media, government regulators, etc.

2.4. Backups

From electrical power to communications and data, every critical business component must have an adequate backup plan that includes:

2.4.1 Data backups to be stored in different locations. This prevents the destruction of both the original and backup copies at the same time. If necessary, offline copies should be kept as well.

2.4.2 Backup power sources, such as generators and inverters that are provisioned to deal with power outages.

2.4.3 Backup communications (e.g., mobile phones and text messaging to replace land lines) and backup services (e.g., cloud email services to replace on-premise servers).

2.4.4 Load balancing business continuity

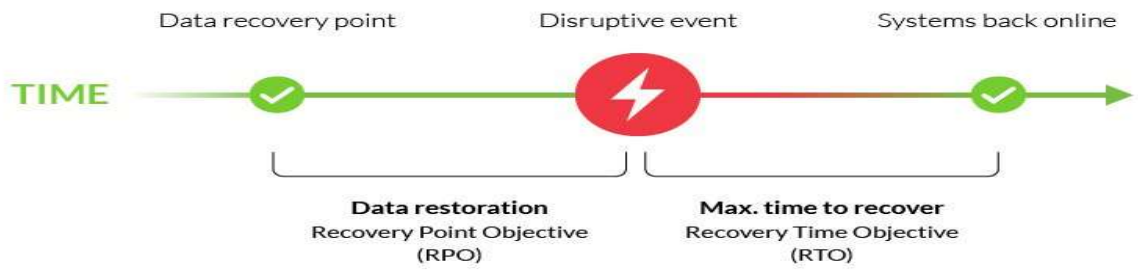
Load balancing maintains business continuity by distributing incoming requests across multiple backend servers in your data center. This provides redundancy in the event of a server failure, ensuring continuous application uptime.

In contrast to the reactive measures used in failover and disaster recovery (described below) load balancing is a preventative measure. Health monitoring tracks server availability, ensuring accurate load distribution at all times—including during disruptive events.

2.5 Disaster recovery plan (DCP) – second line of defense

Even the most carefully thought out business continuity plan is never completely foolproof. Despite best of efforts, some disasters simply cannot be mitigated. A disaster recovery plan (DCP) is a second line of defense that will enable us to bounce back from the worst disruptions with minimal damage.

As the name implies, a disaster recovery plan deals with the restoration of operations after a major disruption. It's defined by two factors: RTO and RPO.



2.5.1 Recovery time objective (RTO) – The acceptable downtime **f**or critical functions and components, i.e., the maximum time it should take to restore services. A different RTO should be assigned to each of your business components according to their importance (e.g., ten minutes for network servers, an hour for phone systems).

2.5.2 Recovery point objective (RPO) – The point to which your state of operations must be restored following a disruption. In relation to backup data, this is the oldest age and level of staleness it can have. For example, network servers updated hourly should have a maximum RPO of 59 minutes to avoid data loss.

Deciding on specific RTOs and RPOs helps clearly show the technical solutions needed to achieve your recovery goals. In most cases the decision is going to boil down to choosing the right failover solution.

2.6 Choosing the right failover solutions

Failover is the switching between primary and backup systems in the event of failure, outage or downtime. It's the key component to disaster recovery and business continuity plans. A failover system should address both RTO and RPO goals by keeping backup infrastructure and data at the ready. Ideally, failover solution should seamlessly kick in to insulate end users from any service degradation.

2. Before Disaster Procedures:

- Keep important phone numbers stored in cell phones

Service	Service vendor	Contact Numbers
Computer/hardware vendor	Kepri Computers	9322915299
Computer software vendor	Comtek	67997887-8
Call Recording	Technitel	9225773886
NSE Lease Line	TATA TELE	18004199963
BSE LeaseLIne	Tata Telecom	022-22722424
BSE Helpdesk	BSE	02230594000
NSE Helpdesk	NSE	1800260050
CDSl HelpDesk	CDSL	022-23058642
Website	Webzol	022-28951271
Phone Line Provider	Airtel-HELP-MAN	9773611004

- Determine a specified meeting place in the event that the office is destroyed or inaccessible.
  Meeting Place Registered office: 631, P J Towers, Dalal Street, Fort, Mumbai. 400001
- Determine which employees are responsible for making critical phone calls during a disaster.

Name of Employee	Work assigned	Staff Contact Number
Vinod Gujar	Back office Software restoration from Back-up storage disk	9967414012
Vinod Gujar	Hardware System availability through Kepri Computers	9967414012
Mansi	Co-ordination with clients/messaging	9768648868
Sarika and Smita	Restoration of DP- system	9892694391
Vishal	Followup with NSE/BSE Leaseline & Activation of alternate trading platform	9322229182
Bhavesh	Restoration of accounts data	9773216495
Raj Mangal	Contact phone line provider Call Broadband Internet provider Contact call recording vendor	8355846791

- Determine where a temporary office location would be.
  Company office at: 814, P J Towers, Dalal Street, Fort, Mumbai. 400001
- Configure Email at employee's homes so that it is functional (or at least able to view old messages) if the network is down.
- Implement a thorough off-site backup system
  System In place at company office: 814, P J Towers, Dalal Street, Fort, Mumbai. 400001
- Store all important software and licenses off-site. Implement a procedure to continually update the off-site library.

Done through Computer Vendor- Kepri Computers

- Thoroughly document all network settings, and keep up-to-date and off-site.
  BSE trading connectivity: through BSE LAN system at 814, P J Towers, Dalal Street, Fort, Mumbai. 400001
  NSE trading connectivity: through net based BOW platform
  CDSL trading connectivity: through BSE LAN system
- If the web site is hosted locally, determine where it can be temporarily hosted elsewhere.
  Through Website maintenance vendor- Webzol
- Quarterly, updating of a USB Flash drive for each department head to keep off-site, which contains the following:
  - A current contact list (home phone number, cell phone number, and family contact) for all employees and management.
  - An updated contact list of customers.
  - An updated contact list of vendors.
- Annually:
  - Take an inventory of hardware that might need replacing in a disaster- done by vendor Kepri Computer
  - An updated contact list of customers- done on a separate mobile phone meant only for customers' correspondence
  - Hold a meeting where you discuss the BCP with your employees.

3. After Disaster Plan procedures:

- Relocate to our alternate office space: 814 P J Towers, Dalal Street, Fort, Mumbai. 400001.
- Check for BSE, NSE and CDSL connectivity at 814, P J Towers, Dalal Street, Fort, Mumbai. 400001
- All staff to be reminded and apprised of their assigned duties
- Call insurance company.
- Call hardware Vendor- Ordering new servers, switches, Internet, Racks, workstations, etc
- Call Software vendor- Restoring company data to the pre-determined computer
- Call your phone line provider. Forward main line to someone's cell phone
- Call- phone recording vendor- Order a new phone system or move to a Hosted PBX service
- Call your broadband ISP- get the connectivity restored.
- Email all customers (using personal Email address if necessary) about the situation; Customers would have to call cell phones; give out a temporary address to send payments if necessary.
- If fire:
  - Arrange to hold mail at the Post Office until the address can be changed.
  - Order office furniture and supplies if necessary.

4. Password Policy

Password policies should continue to evolve even if user attitudes don't. Experts suggest placing more emphasis on checking passwords against known weak password lists and focusing less on password expiration policies. We've encapsulated some advice to formulate our own policy and practices in use:

- Set complexity requirements, such as meeting a character minimum, and use certain character types (mixed case, numerals, and special characters).
- Prevent users from choosing previously used passwords.
- Require passwords to be changed periodically and perhaps frequently.
- Check passwords against lists of most-common or especially weak passwords.

Password requirement at the following levels:

Type of system	Access to /Person in charge	Password Policy to be followed
NEAT	Respective Dealers	• To be set as per NSE policy. Mix of alphanumeric and special characters. Alphabets to be in both small and large faunts. • Password change – as per NSE policy • Password to be saved in protected excel or Note pad file
BOLT	Respective Dealers	• To be set as per BSE policy. Mix of Alphanumeric and special characters • Password change – as per BSE policy • Password to be saved in protected excel or Note pad file
BACK OFFICE SERVERS	Vinod Gujar	• To be set as a mix of Alphanumeric and special characters. Alphabets to be in both small and big faunts • Password change – weekly • Password to be saved in protected excel or Note pad file
Back office desktop PCs	Respective staff in charge	• To be set as a mix of Alphanumeric and special characters. Alphabets to be in both small and big faunts • Password change – weekly • Password to be saved in protected excel or Note pad file
Website Passwords	Respective departments	• To be set as a mix of Alphanumeric and special characters. Alphabets to be in both small and big faunts • Password change – weekly • Password to be saved in protected excel or Note pad file
Banks: login and transaction passwords	Management/directors	• To be set as a mix of Alphanumeric and special characters. Alphabets to be in both small and big faunts • Password change – weekly • Password to be saved in protected excel or Note pad file

5. IT Access Version Document

Our IT Access Control Policy is assigned the version in the following format: NNN.VV/YYYY.

Where NNN = stands for number

V V= version change during the year

YYYY = stands for the FY (financial Year) in which the policy was made.

So the first policy for the year 2020-2021 should be nomenclated as 001.01/2020

And subsequent change in versions during that FY should be nomenclated as 001.02/2020

Document Control

Document title **IT Access Control policy**

Version History

Version No.	Version Date	Author	Summary of Changes
001.01/2020	01.04.2020	K M Jain Stock brokers Pvt Ltd	NA
001.02/2020	01.09.2020	K M Jain Stock Brokers Pvt Ltd	NA

Approvals

Name	Title	Date of Approval	Version No
K.M.Jain Stock Brokers Pvt Ltd	IT Access Control policy	01.04.2020	001.01/2020
K.M.Jain Stock Brokers Pvt Ltd	IT Access Control policy	01.09.2020	001.02/2020

Distribution

Name	Title	Date of Issue	Version No
K.M.Jain Stock Brokers Pvt Ltd	IT Access Control policy	02.04.2020	001.01/2020
K.M.Jain Stock Brokers Pvt Ltd	IT Access Control policy	02.09.2020	001.02/2020

6.Organization Chart- K M Jain Stock Brokers Pvt Ltd