# ORGANIZATION ACCESS AND DISASTER POLICY

**Introduction**

In order to manage the unforeseen disaster and to come out of the ill effects of the same with least damages to business, business continuity plan (BCP) and Disaster Recovery Plan (DRP) is in place. It becomes a guideline for the company to see through the ill facade of business uncertainty.

These two plans complement each other and through our organization's constant review of business and system processes, the plans are updated to match size of business and its growth. The plan is created keeping in mind the business operation locations and risks.

Contingency plans stated are active. Issues relating to routine operations, electronic or communication failures are dealt with as part of Business Continuity Plan where as issues relating to natural calamities like earthquake, flood, fire or any other natural or disaster due to human error are dealt under DRP Plan.

**Objective of Surveillance:**

- Business Process Continuity ensuring desired level of efficiency.
- Maintenance of business data integrity &confidentiality.
- Maintaining data security.
- Speedy retrieval of data and other operational aspects thus allowing for minimum down time and optimum customer satisfaction.

**Areas of Surveillance**

**Physical Surveillance of IT assets:**

- The building premise is equipped with 24 hour security guard surveillance.
- Maintain proper location of system so that unauthorized access by third parties does not happen.
- The main gate of the office premises is secured with physical locks.
- Always ensure that third party vendor is accompanied into the server room and activities monitored.
- Office premise is equipped with 24 hour audio and video surveillance to record and monitor any unusual activities taking place in the organization.

**Data:**

- ODIN Manager and Database Server – Backup taken on a daily basis.
- Database Restore Process - Menu screen shots, option selection and steps till completion of process is provided in manual format earmarked as DR.

**User responsibility & accountability:**

- User management norms are defined and observed as per respective exchange regulations and circulars issued from time to time.
- Password policy/standards are defined and observed as per respective exchange regulations and circulars issued from time to time.

**Maintenance and upgradation of hardware and software:**

- Testing of UPS performance, battery and DG set are carried out on a quarterly basis.
- All staff is strictly instructed not to keep any inflammable items upon any electrical systems.
- Staff is instructed to keep their desks/working environment clean and dust free.
- A list of contact numbers is made available for emergencies.
- We also propose to permit entry to the server room only by introducing the "Secured Electronic Identification" by means of Smart Cards.

Business processes are to be performed in adherence with the policies and procedures defined by authorities and exchanges. These practices are suitably changed as per circulars/directives on a continuous basis.

**Business process contingency:**

- For maintaining uninterrupted connectivity in online trading we have installed two internet lines.
- If connectivity failure of any of the above two lines are reported, the affected clients are reconfigured to connect to the other line.
- ODIN registry files are available on FTP site, company website and also made available to all the clients at the time of installation.

- Antivirus and firewalls are to be updated with the latest patches on a regular basis. Renewals and subscriptions are also to be renewed on a timely basis to allow uninterrupted service to customers.

**Surveillance:**

Preventive: Daily Start-up process Status report is monitored.
Detective: All server events are monitored a daily basis.
Corrective:

- Clients are guided through the menus by the helpdesk staff to ensure smooth uninterrupted running of the programs. Various helpdesk staff are allotted specific call support task, customer complaints, installation and troubleshooting over phone or through email.

- These activities are monitored as per escalation procedure separately. The same is informed to all through circular/email.

**Plan Drill**:

- Backup restoration is tested quarterly basis.

- Backup connectivity is tested every month.

- Management conducts surprise visits in IT functions to confirm that no unauthorized person has any access to the IT setup.

- Loose data cables and loose electrical wires are monitored/segregated to avoid disruption to operation.

- Process is reviewed at regular intervals to ensure that downtime is minimized and operations are updated regularly.

**Capacity Management:**

- We have close monitoring on hardware performance. We allow CPU usage to edge 50%. Hardware is upgraded as and when requirement is arisen. Server hardware, routers, switches are housed on proper racks and access to area is restricted to authorized personnel.
- The capacity is properly airconditioned.
- The capacity is equipped with UPS system having power backup for uninterrupted business operations.
- We have designated third party agencies as well as in-house personnel to maintain hardware as well as software resources.

- We also continuously monitor the performance all hardware installed in the office and we have policy to replace unserviceable hardware on regular basis.
- We also continuously review and compare hardware capability and capacity with reference to our growth plan and present volume of activity. The necessary modifications (if any) of hardware is done as and when required.

**Business Continuity Plan**:

We have ensured to create a setup capable of handling current operations for business contingencies and continuity plan.

We have planned for growth in the years to come and its requirement. The monitoring, restructuring, re-defining of network requirement, hardware requirements and software requirements is being done continuously in consultation with in-house IT team sitting at all office locations and third party agency.

We have appropriate hierarchy of management personnel and executives providing continuous training and giving right kind of exposure to employees. We have regular monitoring and provision of training and development of our staff. We strive to maintain positive and willing atmosphere for all employees allowing them to grow simultaneously.

We also have created business organization required for sincere needs with reference to the envisaged growth and sourcing or equipping our selves by hiring outside experts either on full time basis or on retainer basis to ensure that business continues in all circumstances.

We keep vigil on market movements and consider expert advice on market movements to safeguard our branches and clients allowing them to keep manageable exposure in the market.

We aim to remain competitive in offering our services to our clients and have kept vigil on market development in brokerage and depository service charges. We provide assistance to clients on any investment related issue, queries related to internet trading, global market view and basic understanding of the market.

**Disaster Recovery Plan (DRP)**

**A. Preamble**

This plan document is the only document that replaces/over rules all the past instructions issued by various officials in so far as that conflicts with the present plan.

If and when NSE/BSE/MCX/NCDEX issues any instruction to broking member with reference to the domain of this plan and if the same conflicts with the laid down plan, then the Exchange or other statutory authorities rule shall be binding and DRP plan shall be modified suitably to incorporate such changes.

The following DRP plan is adopted by RELITRADE.

**B. Plan Follow up Yardstick**

Plan status categories are:

- Plan In Place
- Action Plan to be implemented
- Plan for follow-up and surveillance

**C. Plan**

1. The Plan in place is as follows:

a) Standard office floor layout plans take care of the unforeseen disasters, physical access risk to IT and other resources from visiting third parties and clients.

b) HOD system is assigned the duty to manage the affairs at the time of crisis and co-ordinate with other team members and external agencies.

c) Exchange's Mock Trading session are conducted on the backup server.

d) Emergency contact nos. of important utility functions and functionaries are displayed at HO.

e) No-Smoking policy is strictly enforced at HO.

f) Old data should be preserved for a period of at least 1month.

g) Regular media backups are to be taken and kept at off site location.

h) Preventive test of the UPS system and its battery load by switching off Mains to be conducted at timely intervals.

i) HO floors have no recent water damage evident on the walls, floors or ceiling arising out of plumbing leakage, leakage from mainframe water cooling systems or air conditioner.

j) Water, sewer or drain-pipes do not pass through ceiling or walls of the system room of HO.

k) Hard copy of the latest emergency passwords for servers, routers etc. are stored at off-site with the top officials of the company.

l) HO is to strictly adhere to password secrecy policy for servers and all user IDs.

m) There are no instances of disaster happening at the HO or its neighborhood in recent past.

n) There is no proximity to a center storing or dealing with hazardous materials nearby. There are no reports of any fire or noxious fumes anticipated near the HO.

o) No contaminations are spread in the environment from within the premises or neighborhood.

p) The area is politically or for other social factors not disturbed in the past and area is not affected by civil disorders occasionally leading to riots/firing/bombing etc.

q) Server room, office maintenance and cleaning carried out at regular intervals.

r) The roofs of the HO are sound and not dampening.

s) Cabling for electrical installation at HO is hidden/safe.

t) Network cable line has been drawn separated from the electrical cables.

u) The HO building has proper drainage facility and business being located at sixth floor inundation risk is remote.

v) Power and surge protection requirements have been identified and adequate surge protection devices have been installed.

w) Power-lines are kept in three phase which is as per prevailing standard of safety. (One phase for computer with UPS, second for AC and other high power consuming devices like fans and coolers and the third for lights).

x) Periodic checking is carried out to ensure that overloaded outlets within the HO for any of the phase to be identified and remedied immediately upon identification.

y) Server room access is prevented for third party vendors without authorization. Server room access is totally restricted for any other visitor. Appropriate server room access control measures for employees are followed. UPS, hardware, software vendors are always escorted to server room and their activities monitored and reported to HO System.

z) Security of the premises during off-hours is satisfactory.

2. **Action Plan to be implemented:**

The Emergency Contact Nos. should be displayed at HO for systems personnel, service engineer of FT, operating systems, hardware, UPS system, communication service providers, electrician, electricity company complain no, disaster central team members.

Develop Management Information System (MIS) which incorporate summary of business operations and its core activities. This involves details from all divisions i.e. IT, Accounts, Operations, demat, etc.

3. **Plan for follow up and surveillance**:

Risk and impact on business: HO to conduct in-house meeting every month to assess minimum critical time required to resume business in case of business interruption under various scenarios like natural calamity (flood/EQ/fire), manmade calamity (riot, arson) or electronic calamity (server crash, communication line down, electronic fraud). The summary of meeting is to be communicated via email or telephone to the DRP team.

The DR plan directive in the form of a questionnaire is to be circulated to review risk.

To monitor second level of checking of critical data and other system generated reports/statements.

HO to conduct situation based drills and discuss disaster prevention awareness program with the staff once every six months.