VINOD SHARES LTD.

Business Continuity & Contingency Plan

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) have been in place. Now it becomes a master document for the company to see through the ill façade of business uncertainty.

These two master plans, which are put into use complement each other and through our organization's constant review of business and system processes, the plans shall get updated commensurate with the size of business and its growth. The plan has been arrived at after making detailed risk evaluation of the location(s) where from the businesses are operated.

MOTTO: Contingency plans stated both, as part of BCP & DRP is active and fault-free. The plans relating to minor or routine electronic or communication failures are dealt with as part and parcel of Business Continuity Plan while contingency plan for the organization for severe calamites like Earthquake, Flood, Fire or any other natural or man made disaster are dealt with under DRP Plan.

Objective of Surveillance:

- Business Process Continuity ensuring desired level of efficiency
- Continuity of Business Data integrity & confidentiality
- Data Security
- Speedy retrieval of data and other operational aspects.

Areas of Surveillance:

- **Physical Surveillance of IT assets-**
  - 24-hour building security guard
  - Maintain proper location of system so that unauthorized access by third parties do not happen
  - Ensure proper physical lock of main gate and server room and restrict admission into server room to other employees not entrusted with any server room management related task
  - Improve upon the systems through in-house maintenance.
  - Always ensure that third party vendor is accompanied into the server room and activities monitored.

- Connectivity:
  - We have two alternatives sites from where the connectivity can be availed, in case the connectivity at any place is not available.
  - The branches get connected either through NOW or dedicated leased lines, or local branches get connected through dial up (ISDN/PSTN) and also through Broad Band.

- Data:
  - ODIN Manager and Database Server –Back up is taken.
  - **Backup Schedule:**
  - Odin database backup process-
  - Backup plan consist of taking backup with reference to following system or data base:-
  - Daily Database Backup Report containing all the six types of daily backup as above, person taking backup to sign and the same signed by another who verified it and note down to whom media is handed over (in Implementation stage)
  - 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 defined and observed as per respective exchange regulations and circulars issued from time to time.
  - Password policy/standards defined and observed as per respective exchange regulations and circulars issued from time to time.

- Change Control Management:
  - Management desires that as the business is new and growing, in keeping with growth, shall maintain numbered Change Request Form (CRF) for all requests changes in software submitted to Financial Technologies or other software vendors.
  - System Administrator maintain record of all the versions and patches installed for various OS and application from time to time for
    - HO
    - Branch
    - Retail Clients

- Maintenance and up gradation of hardware and software
  - Verification of UPS and Battery and Generator Set on a quarterly basis is introduced

- Each staff is strictly warned not to put any inflammable item upon any electrical systems
- To make the environment dust free.
- A call list for the emergencies
- The physical access by only authorized employees is introduced.
- We also propose to permit entry to the server room only by introducing the "Secured Electronic Identification" by means of Smart Cards.
- We are in the process of equipping the entire company against fire hazards and shall install suitable fire fighting equipments.

- Preparation, Maintenance and Revision of documentation: of various critical system processes by itself is identified as one of the critical resource to switch to contingency plan or to avert electronic blunders preventing business disruption.
  - Application System (Documentation is done for Day Begin processes, Data restore, Data Backup Process, Escalation for response to email)

- Escalation Process shall be practiced in the following order:
  - In case of Day Begin or Day End Failure:-..
  - Other System processes failure:

- Business Processes are to be performed strictly in adherence with the policies and procedures defined by various authorities and exchanges and the practices are suitably changed as per circulars/directives on a AS IS basis before deadline.
- Business process contingency:
  - For online trading no of internet lines-2
  - If connectivity failure of any of the above tow lines are reported, the affected clients are called back to reconfigure client machine IP to switch over to the other line.
  - ODIN registry files are available on ftp site and available to all the clients
  - These files can be downloaded at client systems and continue trading.
  - Antivirus and firewalls are to be updated on an online basis.

- Critical Processes Management:
  - Server Startup Process – menu screen shots, option selection and steps till completion of each of the processes is provided in Manual Format

Surveillance:-

- Preventive :
  - Daily Start-up process Status report is monitored
- Detective:
  - All Server's Event viewer monitoring is done on a daily basis
- Corrective:
  - Usually 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 specific to the job domain of the staff and customer complaints received over phone or through email are monitored as per escalation procedure separately explained elsewhere. The same is informed to all through circular/email.
- Plan Drill
  - Backup Restore Plan is tested regularly.
  - Backup connectivity as available is tested every month.
  - Management's Surprise visits to various IT locations to confirm that no stranger has any access to the IT setup.
  - Loose data cables and loose electrical wires are closely monitored.
  - Whole plan is regularly reviewed to ensure that plan is modified with the change in processes and documentation is accordingly revised.

- Capacity Management

- We have close monitoring on hardware performance. We allow CPU usage to edge 50%.Hardware is upgraded as soon as CPU usage edge over 50% for reasonable time period. Server hardware, routers, switches are housed on proper racks and access to area is controlled. The capacity is properly air conditioned. We have designated agencies to maintain hardware as well as software resources.

- We also continuously monitor the performance of each and every hardware installed in the office and we have policy to ensure to replace unserviceable hardware on regular basis.

- We also continuously review and compare hardware capability and capacity with reference to our growth plan and the present volume of activity and accordingly modification replacement of hardware is being done.

VINOD SHARES LTD.

- Risk Management (Policy Document)

  - We have installed ODIN as affront-end and also use NEAT wherever required. Both these software are provided with controllable risk parameters.

  - We have online real-time basis risk management software with well defined parameters installed in our trading system provided by outside vendor who has provided similar software and proven functioning of the same.

  - The risk parameters are the very well defined by the Chairman & Managing Director and the risk management team sitting at Head Office .The executive personnel do not any authority to change any risk parameters defined and instructed to them and installed on the software.

  - Further, the trade surveillance and monitoring of trading activities of different constituents connected to our main server is being viewed on continuous basis and alerts, warnings are sent to the erring constituents immediately and corrective actions are taken instantly.

  - Further, strict monitoring and follow-ups is being kept on all the branches after day end reports and any warnings or correction in security parameters on the risk management software is required with specific branch or a client is taken before day end.

  - Further, the analysis of trading activity of major clients is being regularly done to ensure that no risk of bad debts or faulty activity is carried out by any constituents.

VINOD SHARES LTD.

Disaster Recovery Plan

A. Preamble

This plan is to be known by the short name DRP. This plan document is the only approved 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/MCDX/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.

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
   I. The Broker has initiated DRP plan since the inception of broking business.
   II. 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.
   III. For each branch, the branch-head is responsible to interact with Central DRP team and follow DRP Plan implementation and surveillance. Crisis Management at branch is handled by branch head.
   IV. The Branch-In-Charges are communicated of their DRP task by the Central DRP team members.
   V. HOD System is assigned the duty to manage the affairs at the time of crisis and coordinate with other team members and external agencies.
   VI. Exchange's Mock Trading session is conducted always on the backup server.
   VII. Emergency contact Nos. of important utility functions and functionaries are displayed at HO.
   VIII. NO-Smoking policy is strictly enforced at HO and branches.
   IX. HO and branches to maintain insurer's policy no, branch location, contact address, telephone and fax nos. which is required for lodging claim intimation.

X. Online Data Backup of Branch's critical data to be daily taken by HO
XI. Policy for preservation of old data is in place.
XII. Regular Media backups to be taken and kept at off site location.
XIII. Preventive test of the UPS system and its battery load by switching off Mains to be conducted
XIV. 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.
XV. Water, sewer, or drain-pipes do not pass through ceiling or walls of the system room of HO.
XVI. Hard copy of the latest emergency passwords for servers, routers etc. are stored at off-site with the top five officials of the company
XVII. HO and Branch strictly to ensure password secrecy policy for servers and other user IDs.
XVIII. There are no instances of disaster happening at the HO/ branch or its neighborhood observed in recent past.
XIX. There is no Proximity to a center storing or dealing with hazardous materials and there is no risk of any fire or noxious fumes anticipated from neighborhood for HO and branches.
XX. No dust or other contaminations are spread in the environment from within the premises or neighborhood
XXI. 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.
XXII. Computer room maintenance and cleaning carried out at regular intervals
XXIII. The floor's roof at HO is sound and not dampening.
XXIV. Cabling for electrical installation at HO is safe
XXV. Network cable line has been drawn separated from the electrical cables
XXVI. The HO building has proper drainage facility and business being located at first and third floor, inundation risk is remote
XXVII. Power and surge protection requirements have been identified and adequate surge protection devices have been installed
XXVIII. 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)
XXIX. Periodic checking to ensure that overloaded outlets within the HO/Branch for any of the phase to be identified and remdied.
XXX. 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 vendor is always escorted to server room and their activities monitored and reported to HO System.

XXXI. Physical security of the premises during off-hours is satisfactory

2. Action Plan to be implemented

I. The Emergency Contact Nos. should now be displayed at branch for HO-systems personnel, Service Engineer of FT, Operating Systems, hardware, UPS system, Communication service providers, Electrician, Electricity Company Complain no, Disaster Central Team Members.

II. Branches to ensure adequate UPS battery backup or else Standby generator set of required capacity

III. Fire suppression capabilities such as necessity of fire extinguishers to be evaluated for its utility in the present location after due consideration.

IV. Communication line between the branch and HO is working satisfactorily. Efforts are targeted to ensure backup communication line for branch and HO. The available backup communication line for branch and HO is tested to ensure that the same is working properly

V. Periodic inspection of all electrical devices, extension cords, electrical wiring etc., is carried out.

3. Plan for follow up and surveillance

I. Risk and Impact on Business: Branches to conduct in house meeting in the 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), man made calamity (riot, arson) or electronic calamity (server crash, communication line down, electronic fraud) and clearly communicate the same to Central DRP team.(2). The DR Plan directive in the form of a questionnaire is to be circulated to review risk at each branch locations

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

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

IV. Branches to ensure adequate UPS battery backup or else Standby generator set of required capacity

VINOD SHARES LTD.

Information Security Policy:

We have introduced the physical controls at server room, back office room by not permitting any unauthorized entry physically.

No visitor is allowed in this area without prior approval and they are not allowed to carry any laptops, pen drives, floppies, cds etc., inside the secured areas.

All employees are not allowed to carry any information in any form from the office while leaving the office. No direct access to Internet is provided to anyone other than authorized persons. All the computers are controlled, their activities are frequently viewed by senior officials time and again to ensure that no pilferage of any sensitive information.

No third party vendors, contractors are permitted in restricted zone. Any meetings with this person if required are held at non secured zone office at the front office.

Physical controls of office premises and facilities:

Physical security guard stationed at the entry point guards the office.

No unauthorized entry is permitted.

Suitable locking arrangements are maintained

The keys remain with senior most directors of the Company. For alternative arrangement, the set of keys are kept at a secured place in vicinity of the office.

VINOD SHARES LTD.

- **Information Security policy and Network Security Policy**

Purpose:

- The purpose of this policy is to out line acceptable use of computer equipment at company. These rules are in place to protect the entire company's team and company. In appropriate use expose risks including virus attack, compromise of network system and service and legal issues.

The Scope:

This policy covers employees, contracters, consultants, and temporaries including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased leased by company.

Policy:

1. The legitimate use of network and reasonable level of privacy is ensured.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

3. This policy recommends that any information that is considered sensitive is Encrypted.

4. Regular Audit of network system is done on periodic basis to ensure the Compliance of this policy.

Security and proprietary information

The interface for information contained on Internet/Intranet/Extranet-related system should be classified as either confidential or not confidential, defined by corporate confidentiality guideline, detail of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor

1. Sensitive, trades secret, specifications, customer lists, And research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep password secure and do not share accounts. Authorized users are responsible for the security of their password and accounts. System level

password should be changed quarterly; user level password should be changed every six month.

3. All PCs, laptop and workstations should be secured with a password protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging off (control-alt-delet for win2k users) when host will be unattended.
4. Use encryption of information in compliance with this policy's Acceptable Encryption use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised Protect laptop in accordance with "Laptop Security Tips"
6. Postings by employees from a company email addresses to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of company, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the company internet/Intranet/Extranet. Owned by company shall be continually executing approved virus scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services)

Under no circumstances is an employee of company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company's owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

VINOD SHARES LTD.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the company.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and the installation of any copyrighted software for which company or the end user doesn't have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server(e.g./ viruses, worms, Trojan horse, email bombs, etc.)
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Making fraudulent offers of products, items, or services originating from any company account.
7. Making fraudulent offers of products, items, or services originating from any company account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are with the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification to this policy is made.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.

12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
14. Providing information about, or lists of company's employees to parties outside the company

Email and Communication Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam)
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email headers information.
4. Solicitation of email for any other email addresses, other than that of the poster's account, with the intent to harass or to collect replies.
5. Use of unsolicited email originating from within company networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by company , or connected via company's network.
6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups(newsgroup Spam)

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

We have introduced the physical controls at server room, back office room by not permitting any unauthorized entry physically.

No visitor is allowed in this area without prior approval and they are not allowed to carry any laptops, pen drives, floppies, cds etc. inside the secured areas.

All employees are not allowed to carry any information in any form from the office while leaving the office. No direct access to Internet is provided to anyone other than authorized persons. All the computers are controlled, their activities are frequently viewed by senior officials time and again to ensure that no pilferage of any sensitive information.