

# ***Business Continuity Planning (BCP) / Disaster Recovery (DR)***

## **Introduction**

Interruptions to business functions can result from major natural disasters such as earthquakes, floods, and fires, or from man-made disasters such as terrorist attacks, riots or war. The most frequent disruptions are less sensational—equipment failures, theft or sabotage.

Business Continuity Planning (BCP Plan), also known as Contingency Planning, defines the process of identification of the applications, customers (internal & external) and locations that a business plans to keep functioning in the occurrence of such disruptive events, as well the failover processes & the length of time for such support. This encompasses hardware, software, facilities, personnel, communication links and applications.




BCP plan is intended to enable a quick and smooth restoration of operations after a disruptive event. It includes business impact analysis, where each critical business function has been reviewed to determine the maximum allowable downtime before causing significant degradation to Total Securities Ltd. (TSL) business operations. BCP plan development includes testing, awareness, training, and maintenance.

The BCP plan also defines actions to be taken before, during, and after a disaster.

## **Purpose**

The plan has been developed to allow for Continuity of Business operations at a minimum level within TSL facilities in Mumbai (Bandra, Kandivali and Malad) and Chennai in the event of an emergency.

## **BCP Objective**

-  Protect personnel, assets and information resources from further injury and/ or damage
-  Minimize economic losses resulting from disruptions to business functions
-  Provide a plan of action to facilitate an orderly recovery of critical business functions

- ✚ Identify key individuals who will manage the process of recovering and restoring the business after a disruption
- ✚ Identify the teams that will complete the specific activities necessary to continue critical business functions
- ✚ Specify the critical business activities that must continue after a disruption
- ✚ Recover critical business functions and support entities
- ✚ Minimize damage and loss
- ✚ Resume critical functions at an alternate location
- ✚ Return to normal operations when possible

### **BCP Committee Members and Contact details:**

<b>Name</b>	<b>Designation</b>	<b>Address</b>	<b>Mobile No.</b>	<b>Email ID</b>
Vijay Vora	Director	1 <sup>st</sup> Floor , Eden Garden, Mahavir Nagar, Kandivali, Mumbai – 400 067	9821113346	<a href="mailto:totalsecurities@gmail.com">totalsecurities@gmail.com</a>
Shyam Bihani	Director	406, Sej Plaza, Marve Road, Malad (W), Mumbai – 400 064	9322231104	<a href="mailto:totalsecurities@gmail.com">totalsecurities@gmail.com</a>
Rajesh Modi	Director	1 <sup>st</sup> Floor , Eden Garden, Mahavir Nagar, Kandivali, Mumbai – 400 067	9322231362	<a href="mailto:totalsecurities@gmail.com">totalsecurities@gmail.com</a>
Deepak Jhanwar	Branch Manager	D/77, New Anaj Mandi, Chandpole Bazar, Jaipur- 302 001	09382935101	jhanwar_deepak@yahoo.com

### **Recovery Management Co-ordinator (RMC)**

Kamlesh V. shah	Director	1 <sup>st</sup> Floor , Eden Garden, Mahavir Nagar, Kandivali, Mumbai – 400 067	9892984465	<a href="mailto:kamlesh.total@gmail.com">kamlesh.total@gmail.com</a>
-----------------	----------	---	------------	--

The BCP Procedure is also sent to their mail ID. In case of emergency committee members can retrieve the data from their mail for acting toward the disaster.

## **Procedure – Business Continuity Plan**

This is a disaster recovery plan for TSL Data. The information present in this plan guides TSL operation & Data management and technical staff in the recovery of computing and network facilities and client data in the event that a disaster destroys all or part of the facilities. The primary focus of this BCP is to provide a plan to respond to a disaster that destroys or severely cripples TSL operation & Data computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Disaster recovery plans are developed to span the recovery of data, systems, links and also include worst case scenarios such as:

1. Loss of access to facility
2. Loss of access to information resources
3. Loss of key personnel who are responsible for performing critical functions

### **Personnel**

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

### **Salvage Operations at Disaster Site**

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site

### **Designate Recovery Site / Alternate site / Backup site**

The Five offices spread across 2 cities in India act as backup sites to each other. Each site is equipped to provide similar working environments as other centers. The offices are interconnected with redundant leased lines and LAN network.

### **Purchase New Equipment**

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The TSL operation will rely upon emergency procurement procedures for equipment, supplies, software, and any other needs.

### **Begin Reassembly at Recovery Site**

Salvaged and new components are reassembled at the recovery site. If vendors cannot provide a certain piece of equipment on a timely basis, then recovery personnel can make

Last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

### **Executive Management Team (EMT)**

This group consists of members of BCP Committee, the Recovery Management Coordinator. The Executive Management Group makes the decision to mobilize the TSL's recovery organization. This decision is based upon their best judgment in determining the extent and impact of the outage.

### **Recovery Management Co-ordinator (RMC)**

The Recovery Management Coordinator (RMC) is the individual who manages the recovery operation. Throughout the recovery process, all recovery teams function under the supervision of the RMC.

### **IT Recovery Group**

The IT Recovery Group manages the computer processing, internal/ external network connectivity and computer support requirements of the recovery effort.

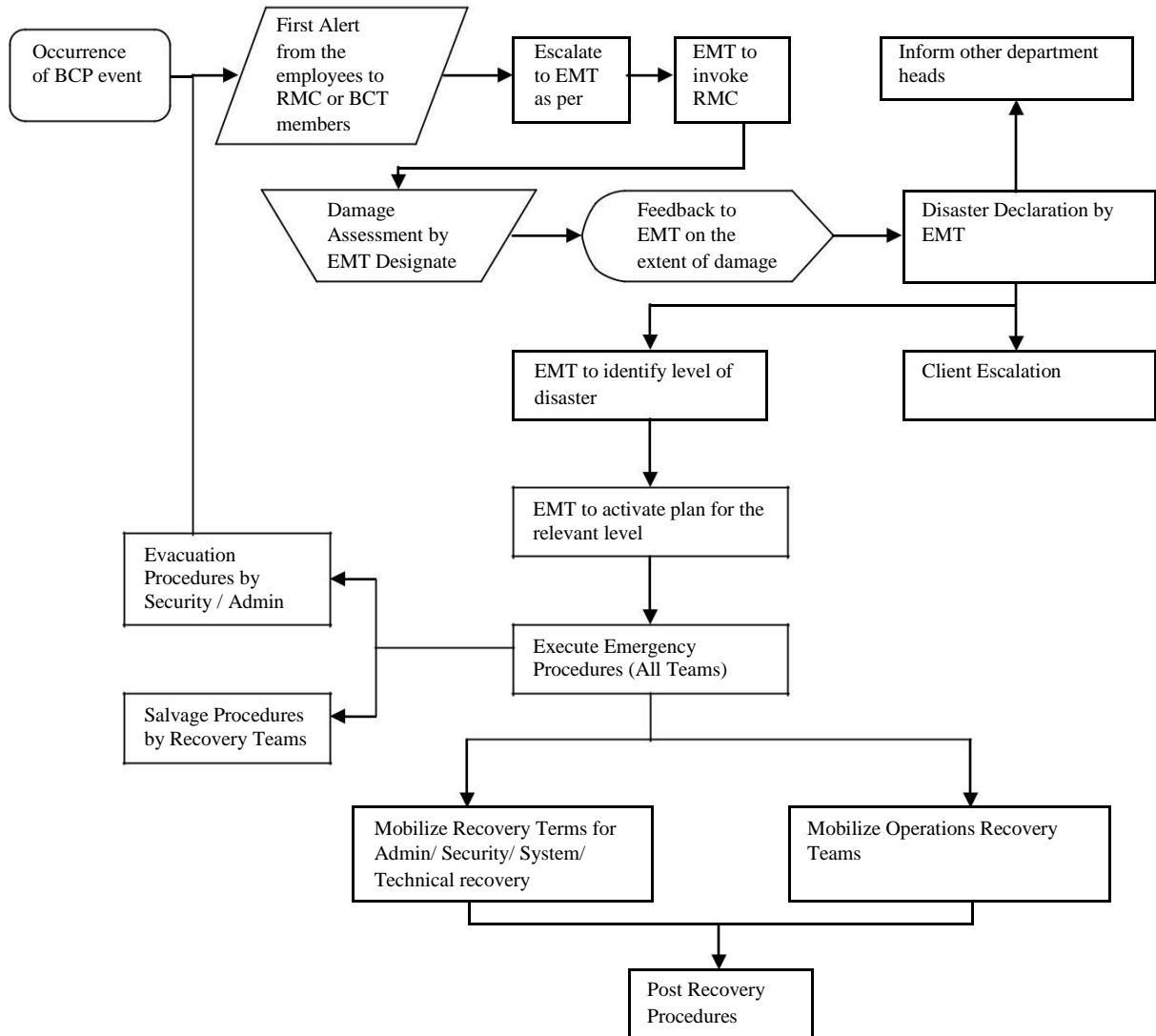
### **Logistics Recovery Group**

The Logistic Recovery Group manages the administrative and logistical requirements of the recovery effort, and performance those duties and activities not directly related to the recovery of business functions.

### **Corporate Communication Group**

Corporate Communication Group is responsible for communication with all TSL employees and clients during recovery operations.

## Total Securities Ltd's Business Continuity Process



### Restore Data from Backups:

Data can be restore from other locations in case of any disaster. And if disaster effect the city as whole say Mumbai then back up data can be restored from other city i.e Chennai and so on.

## **Potential Causes of service interruptions:**

1. Hardware Failure
2. Loss of data/software
3. Failure in communication link components
4. loss of power supply
5. loss / inaccessibility of other location

## **Geared for any eventuality**

<b>Server Hardware Failure</b>	Server to be identified as critical and non critical servers Critical servers to be configured for redundancy for power supply, disk mirroring etc. Redundancy to avoid /reduce impact of server failure.
<b>Loss of Data/ Software</b>	Adequate backup maintained to recover loss of data Weekly backup of database Backup media to be tested at least once in two months Copies of backup maintained in secure offsite location.
<b>Failure in data Circuits</b>	For all communication problems at TSL's end : Equipments (router, connections hub) checked and rectified for problems detected Fully configured backup routers Alternate backup link facility in case of failure in dedicated link in one location
<b>Loss of Power</b>	Uninterrupted power supply through captive power plant UPS system for 2 hrs. to avoid interruption in working.
<b>Loss / Inaccessibility of other location</b>	Square up of position or important client orders can be managed form alternate locations.

## **PREVENTION**

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan

reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created:

- **Fire**
- **Flood**
- **Cyclones and High Winds**
- **Earthquake**
- **Computer Crime**
- **Terrorist Actions and Sabotage**

### **Fire**

The threat of fire in office premises is real and poses *a high risk*. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. The computers within the facility also pose a target for arson from anyone wishing to disrupt TSL operations.

The Building is equipped with a fire alarm system. Hand-held fire extinguishers are placed in visible locations throughout the building. All Staff are trained in the use of fire extinguishers.

### **Flood**

None of the offices are on ground floor, thus risk due to flood is very much limited.

### **Cyclones and High Winds**

Most of the offices are located in Mumbai. Very sever cyclone can only have marginal impact on the operations. Due care and preventive measure appropriate are carried out. Protective plastic cover are available and also operators are trained how to properly cover the equipments.

### **Earthquake**

The threat of an earthquake in Mumbai and Chennai area is medium to low but should not be ignored. Buildings in our area are built to earthquake resistant standards so we could expect least damage from the predicted quake. An earthquake has the potential for being the most disruptive for this disaster recovery plan. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do large scale building repairs.

The preventative measures for an earthquake can be similar to those of a Cyclone. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time.

## **Computer Crime**

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. All systems have security products installed to protect against unauthorized entry. All systems are protected by passwords. All users are required to change their passwords on a regular basis. All systems *should* log invalid attempts to access data, and *the* system administrator reviews these logs on a regular basis.

All systems are backed up on a periodic basis. Physical security of the data storage area for backups is implemented. Standards have been established on the number of backup cycles to retain and the length of their retention.

Policies and procedures are strictly enforced when violations are detected (?). Operators are regularly told the importance of keeping their passwords secret.

## **Terrorist Actions and Sabotage**

Terroristic action and sabotage is potential risk under the circumstances on all the offices in big cities. To prevent such occurrence TSL has system in place whereby each office will permit entry on verification of fingerprint and due care is taken to provide adequate security.



## **Training**

Training seminars addressing business continuity in are conducted on a regular basis. Also awareness programme is conducted to educate management and senior individuals who will be required to participate in the project.

The objectives of Business Continuity Planning training are:

- ✚ Train employees and management who are required to help maintain the Business Continuity Plan
- ✚ Train employees and management who are required to execute various plan segments in the event of a disaster

## **Testing and Evaluation**

The response to each threat situations is tested periodically to assess the preparedness of the organization to execute the recovery plans. Some of the threats that occur frequently, are tested in due course of business, hence are not tested specifically. Others however, require testing and for them a disaster scenario is assumed and the team representatives "walk through" the recovery actions checking for errors or omissions. Persons involved in the test include the Recovery Management Coordinator and members of various recovery teams.

An ongoing testing programme is established. However, special testing is considered whenever there is a major revision to TSL operation or when significant changes in hardware or communications environments occur. The Recovery Management Coordinator is responsible for analyzing change, updating impacts on the plan and for making recommendations for plan testing.

The Team Leaders and the Recovery Management Coordinator review the test results, discuss weaknesses, resolve problems and suggest appropriate changes to the plan.

*An Effective recovery plan is a live recovery plan*  
**Brief Description of BCP / DR Plan**

Disruption	Availability			Impact		Recovery capability
	Processes	Personnel	Technology Assets	Financial	Operational	
Business processes (BP) at TSL level or at any office experience minor damage and will run at a sub-standard level	Adequate	Adequate	Adequate	Low	Low	Immediate
BP at TSL level or at any office may not continue or may run on a sub-standard basis. Alternate equipment or routing of communication links may be required.	Adequate	Adequate	Adequate	Medium	Medium	Hours
Disaster resulting in the total shut down of infrastructure at central office premises leading to shut down of all business process, related infrastructure and non- accessibility of people.	N.A (as there is no central location. Each office is back up for other office)	N.A	N.A	N.A	N.A	N.A
Major disaster resulting in a complete city wide destruction of service and damage to the business centre. Recovery will require the use of an alternate processing site as well as offsite office	Medium	Medium	Medium	Controllable	Controllable	Days

for employees over an extended period of time						
---	--	--	--	--	--	--

- ✚ Identify key individuals who will manage the process of recovering and restoring the business after a disruption
- ✚ Identify the teams that will complete the specific activities necessary to continue critical business functions
- ✚ Specify the critical business activities that must continue after a disruption
- ✚ Recover critical business functions and support entities
- ✚ Minimize damage and loss
- ✚ Resume critical functions at an alternate location
- ✚ Return to normal operations when possible

### **BCP Committee Members and Contact details:**

<b>Name</b>	<b>Designation</b>	<b>Address</b>	<b>Mobile No.</b>	<b>Email ID</b>
Vijay Vora	Director	1 <sup>st</sup> Floor , Eden Garden, Mahavir Nagar, Kandivali, Mumbai – 400 067	9821113346	<a href="mailto:totalsecurities@gmail.com">totalsecurities@gmail.com</a>
Shyam Bihani	Director	406, Sej Plaza, Marve Road, Malad (W), Mumbai – 400 064	9322231104	<a href="mailto:totalsecurities@gmail.com">totalsecurities@gmail.com</a>
Rajesh Modi	Director	1 <sup>st</sup> Floor , Eden Garden, Mahavir Nagar, Kandivali, Mumbai – 400 067	9322231362	<a href="mailto:totalsecurities@gmail.com">totalsecurities@gmail.com</a>
Deepak Jhanwar	Branch Manager	D/77, New Anaj Mandi, Chandpole Bazar, Jaipur- 302 001	09382935101	jhanwar_deepak@yahoo.com

### **Recovery Management Co-ordinator (RMC)**

Kamlesh V. shah	Director	1 <sup>st</sup> Floor , Eden Garden, Mahavir Nagar, Kandivali, Mumbai – 400 067	9892984465	<a href="mailto:kamlesh.total@gmail.com">kamlesh.total@gmail.com</a>
-----------------	----------	---	------------	--

The BCP Procedure is also sent to their mail ID. In case of emergency committee members can retrieve the data from their mail for acting toward the disaster.

## **Procedure – Business Continuity Plan**

This is a disaster recovery plan for TSL Data. The information present in this plan guides TSL operation & Data management and technical staff in the recovery of computing and network facilities and client data in the event that a disaster destroys all or part of the facilities. The primary focus of this BCP is to provide a plan to respond to a disaster that destroys or severely cripples TSL operation & Data computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Disaster recovery plans are developed to span the recovery of data, systems, links and also include worst case scenarios such as:

1. Loss of access to facility
2. Loss of access to information resources
3. Loss of key personnel who are responsible for performing critical functions

### **Personnel**

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

### **Salvage Operations at Disaster Site**

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site

### **Designate Recovery Site / Alternate site / Backup site**

The Five offices spread across 2 cities in India act as backup sites to each other. Each site is equipped to provide similar working environments as other centers. The offices are interconnected with redundant leased lines and LAN network.

### **Purchase New Equipment**

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The TSL operation will rely upon emergency procurement procedures for equipment, supplies, software, and any other needs.

### **Begin Reassembly at Recovery Site**

Salvaged and new components are reassembled at the recovery site. If vendors cannot provide a certain piece of equipment on a timely basis, then recovery personnel can make

last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

### **Executive Management Team (EMT)**

This group consists of members of BCP Committee, the Recovery Management Coordinator. The Executive Management Group makes the decision to mobilize the TSL's recovery organization. This decision is based upon their best judgment in determining the extent and impact of the outage.

### **Recovery Management Co-ordinator (RMC)**

The Recovery Management Coordinator (RMC) is the individual who manages the recovery operation. Throughout the recovery process, all recovery teams function under the supervision of the RMC.

### **IT Recovery Group**

The IT Recovery Group manages the computer processing, internal/ external network connectivity and computer support requirements of the recovery effort.

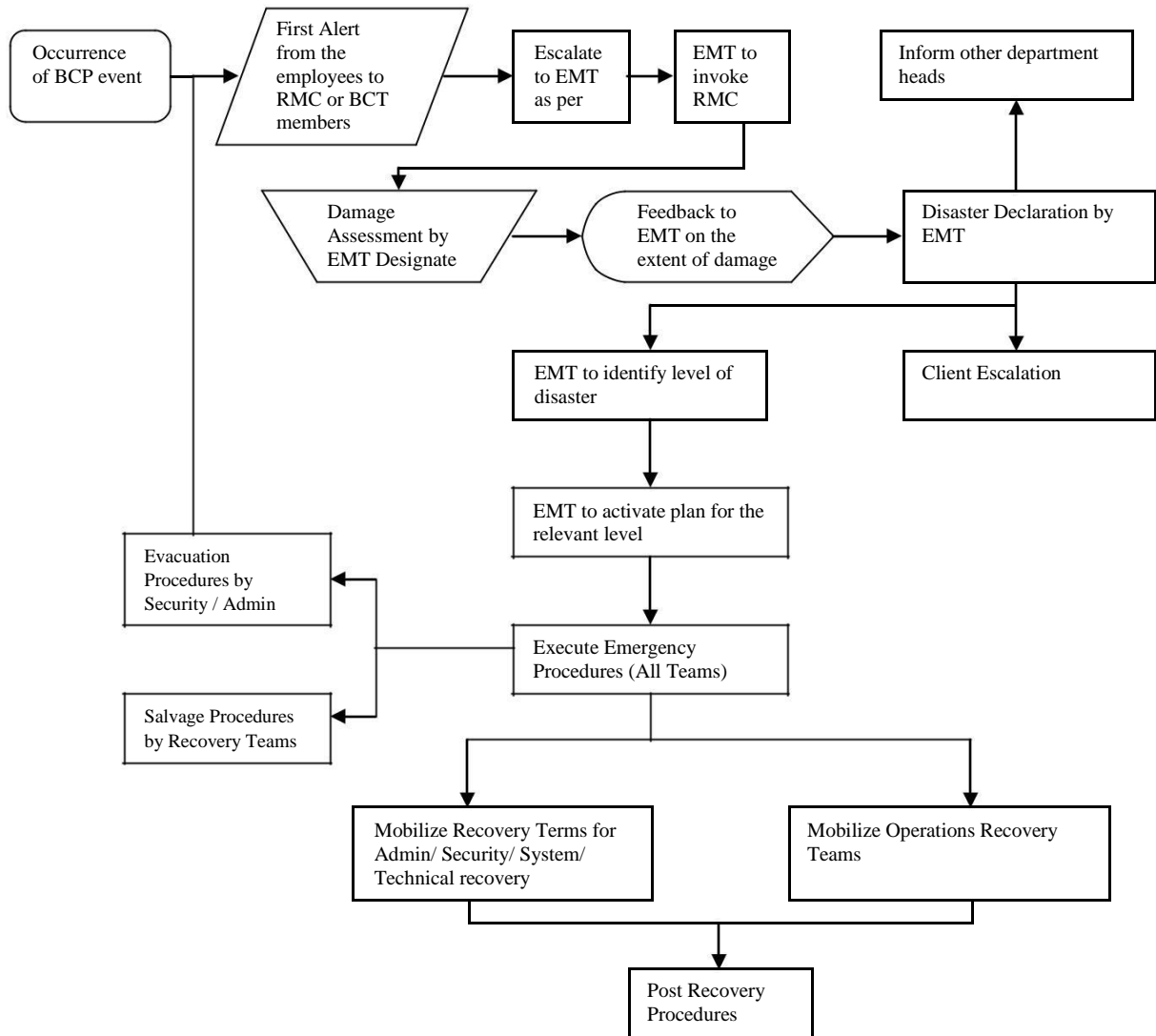
### **Logistics Recovery Group**

The Logistic Recovery Group manages the administrative and logistical requirements of the recovery effort, and performance those duties and activities not directly related to the recovery of business functions.

### **Corporate Communication Group**

Corporate Communication Group is responsible for communication with all TSL employees and clients during recovery operations.

## Total Securities Ltd's Business Continuity Process



### Restore Data from Backups:

Data can be restore from other locations in case of any disaster. And if disaster effect the city as whole say Mumbai then back up data can be restored from other city i.e Chennai and so on.

**Potential Causes of service interruptions:**

1. Hardware Failure
2. Loss of data/software
3. Failure in communication link components
4. loss of power supply
5. loss / inaccessibility of other location

**Geared for any eventuality**

<b>Server Hardware Failure</b>	Server to be identified as critical and non critical servers Critical servers to be configured for redundancy for power supply, disk mirroring etc. Redundancy to avoid /reduce impact of server failure.
<b>Loss of Data/ Software</b>	Adequate backup maintained to recover loss of data Weekly backup of database Backup media to be tested at least once in two months Copies of backup maintained in secure offsite location.
<b>Failure in data Circuits</b>	For all communication problems at TSL's end : Equipments (router, connections hub) checked and rectified for problems detected Fully configured backup routers Alternate backup link facility in case of failure in dedicated link in one location
<b>Loss of Power</b>	Uninterrupted power supply through captive power plant UPS system for 2 hrs. to avoid interruption in working.
<b>Loss / Inaccessibility of other location</b>	Square up of position or important client orders can be managed form alternate locations.

**PREVENTION**

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan



reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created:

- **Fire**
- **Flood**
- **Cyclones and High Winds**
- **Earthquake**
- **Computer Crime**
- **Terrorist Actions and Sabotage**

### **Fire**

The threat of fire in office premises is real and poses *a high risk*. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. The computers within the facility also pose a target for arson from anyone wishing to disrupt TSL operations.

The Building is equipped with a fire alarm system. Hand-held fire extinguishers are placed in visible locations throughout the building. All Staff are trained in the use of fire extinguishers.

### **Flood**

None of the offices are on ground floor, thus risk due to flood is very much limited.

### **Cyclones and High Winds**

Most of the offices are located in Mumbai. Very sever cyclone can only have marginal impact on the operations. Due care and preventive measure appropriate are carried out. Protective plastic cover are available and also operators are trained how to properly cover the equipments.

### **Earthquake**

The threat of an earthquake in Mumbai and Chennai area is medium to low but should not be ignored. Buildings in our area are built to earthquake resistant standards so we could expect least damage from the predicted quake. An earthquake has the potential for being the most disruptive for this disaster recovery plan. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do large scale building repairs.

The preventative measures for an earthquake can be similar to those of a Cyclone. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time.

## **Computer Crime**

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. All systems have security products installed to protect against unauthorized entry. All systems are protected by passwords. All users are required to change their passwords on a regular basis. All systems *should* log invalid attempts to access data, and *the* system administrator reviews these logs on a regular basis.

All systems are backed up on a periodic basis. Physical security of the data storage area for backups is implemented. Standards have been established on the number of backup cycles to retain and the length of their retention.

Policies and procedures are strictly enforced when violations are detected (?). Operators are regularly told the importance of keeping their passwords secret.

## **Terrorist Actions and Sabotage**

Terroristic action and sabotage is potential risk under the circumstances on all the offices in big cities. To prevent such occurrence TSL has system in place whereby each office will permit entry on verification of fingerprint and due care is taken to provide adequate security.

## **Training**

Training seminars addressing business continuity in are conducted on a regular basis. Also awareness programme is conducted to educate management and senior individuals who will be required to participate in the project.

The objectives of Business Continuity Planning training are:

- ✚ Train employees and management who are required to help maintain the Business Continuity Plan
- ✚ Train employees and management who are required to execute various plan segments in the event of a disaster

## **Testing and Evaluation**

The response to each threat situations is tested periodically to assess the preparedness of the organization to execute the recovery plans. Some of the threats that occur frequently, are tested in due course of business, hence are not tested specifically. Others however, require testing and for them a disaster scenario is assumed and the team representatives "walk through" the recovery actions checking for errors or omissions. Persons involved in the test include the Recovery Management Coordinator and members of various recovery teams.

An ongoing testing programme is established. However, special testing is considered whenever there is a major revision to TSL operation or when significant changes in hardware or communications environments occur. The Recovery Management Coordinator is responsible for analyzing change, updating impacts on the plan and for making recommendations for plan testing.

The Team Leaders and the Recovery Management Coordinator review the test results, discuss weaknesses, resolve problems and suggest appropriate changes to the plan.

*An Effective recovery plan is a live recovery plan*  
**Brief Description of BCP / DR Plan**

Disruption	Availability			Impact		Recovery capability
	Processes	Personnel	Technology Assets	Financial	Operational	
Business processes (BP) at TSL level or at any office experience minor damage and will run at a sub-standard level	Adequate	Adequate	Adequate	Low	Low	Immediate
BP at TSL level or at any office may not continue or may run on a sub-standard basis. Alternate equipment or routing of communication links may be required.	Adequate	Adequate	Adequate	Medium	Medium	Hours
Disaster resulting in the total shut down of infrastructure at central office premises leading to shut down of all business process, related infrastructure and non- accessibility of people.	N.A (as there is no central location. Each office is back up for other office)	N.A	N.A	N.A	N.A	N.A
Major disaster resulting in a complete city wide destruction of service and damage to the business centre. Recovery will require the use of an alternate processing site as well as offsite office	Medium	Medium	Medium	Controllable	Controllable	Days

for employees over an extended period of time						
---	--	--	--	--	--	--