IT Disaster Recovery Plan Template

ABC PVT LTD

Primary site
ABC Towers Bangalore India
560047

Secondary site
ABC Towers Delhi India
110059

Aerial distance between sites
1800 KMS

Inter-site connectivity backbone
DWDM

Record of Revisions

The following is a list of revisions made to this document.

Rev	Date	Pages Affected	Person Responsible	Signed Off By
1	04/27/2011	All	Anuj Sharma	

Introduction

This document covers the process and disaster recovery procedures in place at ABC PVT LTD in case of a disaster. The disaster can be a geographical disaster or any other failure that leads to the Production Environment's downtime. The purpose of this document is to ensure minimal downtime, data integrity and availability, in case of a disaster. This document will try to cover all the aspects that should be taken care in case of a disaster, as well as the safety of people. This document outlines the process and procedures that will help us overcome the disaster with minimal effect on the working of our organization.

Emergency Key Personnel Contact Info

Emergency Situation Spokesperson

Name:
Mobile Number:
Home:

Primary Site: India

Category	Name	Contact Option	Contact Number
SAN Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
BURA Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Application Support Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Facilities Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Network Team Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Server Team		Work	
		Alternate	
		Mobile	
		Home	

Category	Name	Contact Option	Contact Number
		Email Address	
		Alternate Email	
External Vendor B		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	

Secondary Site: India

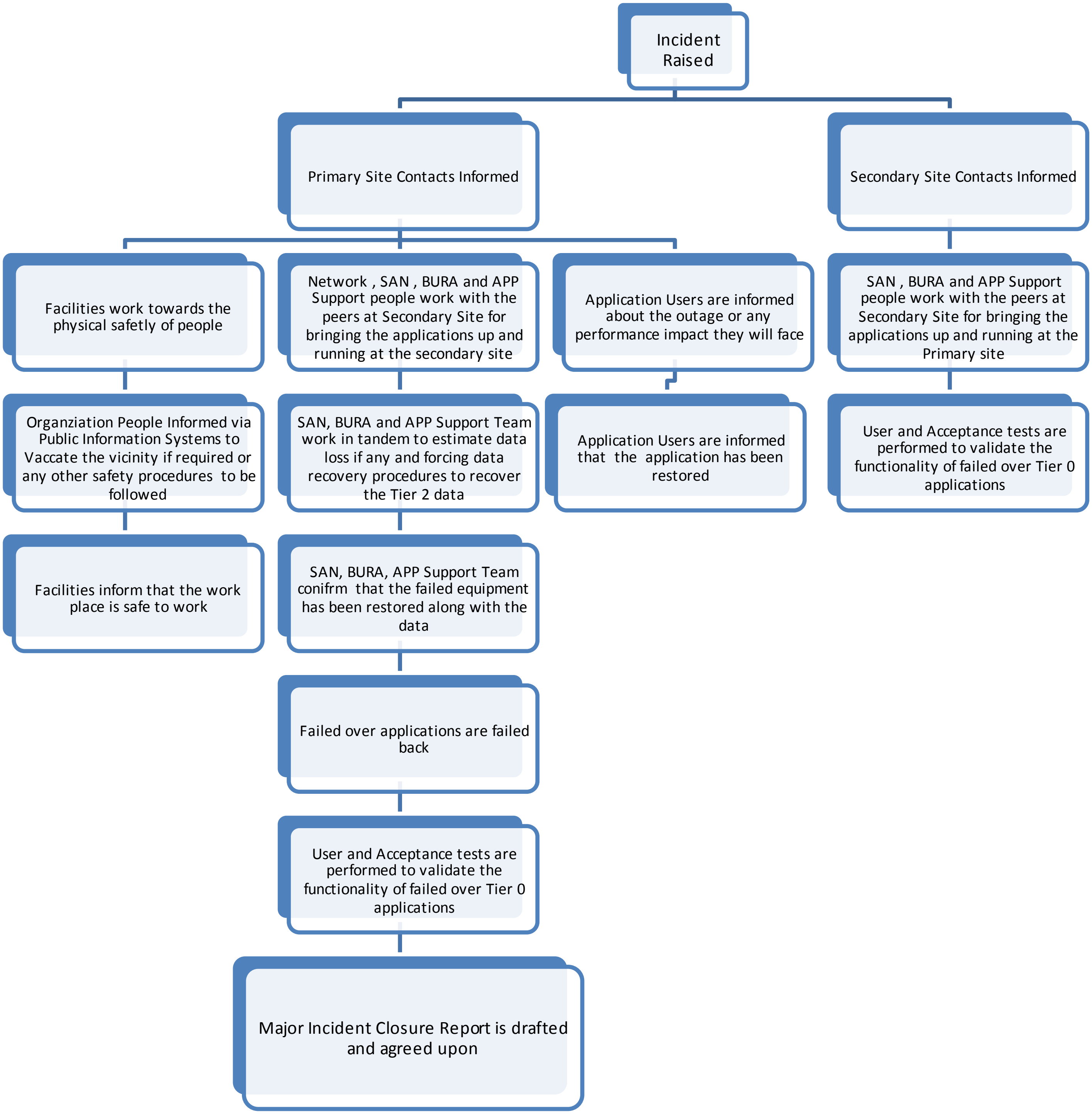
Emergency Situation Spokesperson

Name:
Mobile Number:
Home:

Category	Name	Contact Option	Contact Number
SAN Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
BURA Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Application Support Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Facilities Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Network Team Contact		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	
Server Team		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	
		Alternate Email	

Category	Name	Contact Option	Contact Number
External Vendor B		Work	
		Alternate	
		Mobile	
		Home	
		Email Address	

DR Incident Management Flow



Incident Raised

Primary Site Contacts Informed

Secondary Site Contacts Informed

Facilities work towards the physical safetly of people

Organziation People Informed via Public Information Systems to Vaccate the vicinity if required or any other safety procedures to be followed

Facilities inform that the work place is safe to work

Network , SAN , BURA and APP Support people work with the peers at Secondary Site for bringing the applications up and running at the secondary site

SAN, BURA and APP Support Team work in tandem to estimate data loss if any and forcing data recovery procedures to recover the Tier 2 data

SAN, BURA, APP Support Team conifrm that the failed equipment has been restored along with the data

Failed over applications are failed back

User and Acceptance tests are performed to validate the functionality of failed over Tier 0 applications

Major Incident Closure Report is drafted and agreed upon

Application Users are informed about the outage or any performance impact they will face

Application Users are informed that the application has been restored

SAN , BURA and APP Support people work with the peers at Secondary Site for bringing the applications up and running at the Primary site

User and Acceptance tests are performed to validate the functionality of failed over Tier 0 applications

Data Classification

Server	Application	IP	Connectivity SAN /LAN	Tier 0 / Data Volumes /Data Retention /RPO / RTO	Tier 1 /Data Volumes /Data Retention /RPO /RTO	Tier 2 /Data Volumes /Data Retention / RPO /RTO
Exchange MS	MS Exchange	10.0.1.1	SAN	E:\ 1 year RPO 0 mins RTO 1 Hour	E:\ 1 year RPO 0 mins RTO 1 Hour	C:\ 1 Month RPO- 6 hours RTO-6 Hours
SAPDB	SAP	10.0.1.2	SAN	/root,/var 2 years RPO 0 mins RTO 30 minutes	/root,/var 2 years RPO 0 mins RTO 30 minutes	/local 1 month RPO 0 mins RTO 30 minutes

Equipment Details

Primary Site

	Equipment	Owner Team	Vendor	Serial Number	Support Call Number
Tier 0	EMC VMAX	SAN	EMC	99979797	19810018
Tier 1	EMC Recoverpoint	SAN	EMC	99999999	19808111
	EMC VMAX				
Tier 2	EMC Networker	BURA	EMC		
	EMC DataDomain	BURA	EMC	98289681	1801010010

Server Details

Hostname	IP	Operating System	Application	Backup Tier	DR Server Hostname	DR Server IP	Vendor	Support Contract
Exch01	10.0.0.3	Windows 2008 Enterprise	MS Exchange 2010	Tier0/Tier1/Tier2	Exchdr01	10.0.1.3	HP	Platinum

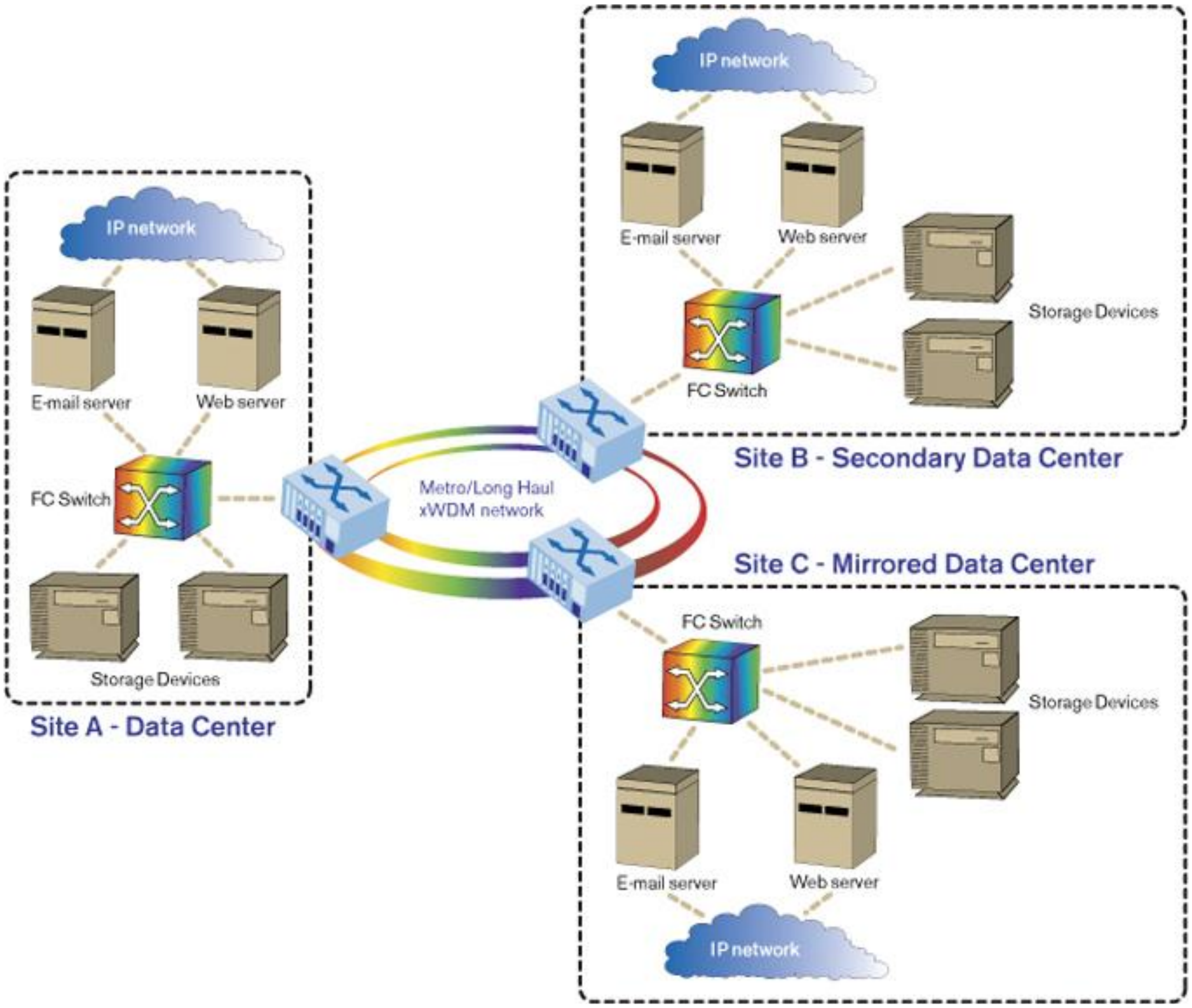
Secondary Site

	Equipment	Owner Team	Vendor	Serial Number	Support Call Number
Tier 0	EMC VMAX	SAN	EMC	99979797	1089011010
Tier 1	EMC Recoverpoint	SAN	EMC	99999999	1801108081
	EMC VMAX				
Tier 2	EMC Networker	BURA	EMC	98989898	18018010810
	DataDomain				

Server Details

Hostname	IP	Operating System	Application	Primary Server Hostname	Primary Server IP	Vendor	Support Contract
Exchdr01	10.0.1.3	Windows 2008 Enterprise	MS Exchange 2010	Exch01	10.0.0.3	HP	Platinum

Disaster Recovery Infrastructure Diagram



Disaster Assessment

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Remedial Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		DR Site
Electrical storms	5		DR Site
Act of terrorism	5		DR Site
Act of sabotage	5		DR Site
Electrical power failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	Two ISP Vendors
Server / Equipment failure	2	3	Redundant Equipment / Cluster Enabled Applications

Probability: 1 = Very High, 5 = Very Low

Impact: 1 = Total destruction, 5 = Minor annoyance

Safe Assembly Area

Opposite Park 5 Tower A

Facilities Emergency Contact Numbers

18000101010
18001001000

Incident Management Process

1. Incident occurred and detected by the Monitoring Procedures in place.
2. Categorize the incident.
3. Incident Report Template opened and updated with the Incident details and the progress.
4. Key Persons informed
5. To avoid panic, regular updates are sent after 30 minutes to affected people about the situation.
6. In case of a disaster at the primary site:
    - People need to be guided to a safe location by facilities team
    - Application users are informed of the outage, if any
    - Secondary Key Contacts need to be notified
    - Emergency Services should be contacted
    - Server, Network, Application, SAN and BURA teams work to resolve the incident
    - In the mean time, Secondary Site time starts bringing up the failed applications
    - User and Acceptance tests are performed
    - Application Users are notified that the application is accessible again
    - Server, SAN, BURA and Application teams work to estimate data loss if any
    - Recover any data that needs to be recovered
    - Facility Team informs that the primary site is safe to work
    - Fail Back of the failed applications is performed
    - User and Acceptance Tests are performed
    - Application performance is monitored for 24 hours
    - Major Incident form is completed and agreed upon by the various owners of the incident
7. In case of a Hardware failure or application failure, respective owners are informed
8. DR procedures in place are put into effect
9. Once the issue with the primary hardware or application is resolved, fail back is done
10. User and Acceptance Tests are performed
11. Application performance is monitored for 24 hours
12. Effected people are informed about the resolutions and step taken
13. Incident is resolved
14. Major Incident form is completed and agreed upon by the various owners of the incident and given final closure by Emergency Situation Spoke Person
15. Any recommendations by the group are forwarded to the upper management along with the incident report to stream line the process further

Major Incident Update Alert

Major Incident

April 13, 2011

Issue

Exchange Offline

Schedule of Outage(s)

System/Application Affected	Start Time of Outage	End Time of Outage
MS Exchange	12:00 AM GMT	15:00 AM GMT

Group Responsible for Work

Server , SAN, BURA and APP Support

Business Impact

Users not able to access MS Outlook

Incident Number

12638638

Next Update:

Regards,

Emergency Incident Management Team

Major Incident Report

Location	**Incident Number**	**Associated Reference Numbers (i.e. Third Party/Client) SR**
Application/Component	**Application/Component Outage**	**Issued Date & Version**
Report Author	**Time/Date Call Opened**	**Time/Date Call Fixed**
Problem Description		

Business Impact

Summary of Events		
Time	**Date**	**Event**

Current status

Post Mortem Actions						
No	Description	Action By	Priority	Target Date	Status	Completed Date

Recommendations