PRAMATI

Business Continuity

&

Disaster Recovery Plan

Version 5.0

Template Revision History

Version Number	Date	Prepared By	Reviewed By	Approved By	Summary of Changes
1.0D1	25-Aug-2011	Sai Krishna	Sairam	Lokesh	
1.0	09-Sep-2011	Sai Krishna	Sairam	Lokesh	
1.0	05-Nov-2012	Mahati	Sai Krishna	Sai Krishna	

Document Revision History

Version Number	Date	Prepared By	Reviewed By	Approved By	Summary of Changes
1.0	10-Nov-2011	Sairam	Lokesh	Lokesh	Added specific Business continuity plans, strategies and processes pertaining to all the important functions and services of Pramati.
1.1	22-Feb-2012	Mahati	SaiKrishna		• Added Emergency evacuation plan in the Test approach • Updated Venu/Ravi mobile numbers in Section 3.6
1.2	01-Nov-2012	Mahati	Sai Krishna	Sai Krishna	• 3.6 Updated with emergency contact list • Qontext, Rajiv, Sairam has been removed in the entire document and updated with latest.
1.3	03-Jun-2013	Mahati	Sai Krishna		Change of address
1.4	08-Oct-2013	Sai Krishna	Sai Krishna	Chandru	Updated contacts & locations Updated dates of Fire Drill conducted
2.0	21-Jan-2015	Pavan K	Rajesh K	Rajesh K	Included section on conditions for activating the BCP plan, detailed activities of BCP, Technology Availability Plan, Disaster scenario analysis plan, BCP Test plan and SLA, Location wise internal and external contact list
3.0	22-Feb-2016	Pavan K	Rajesh K	Rajesh K	Updated BCP contacts, facility non-availability scenario modified for fire brigade and included medical emergency
4.0	13-Feb-2017	Sai Kishore G	Rajesh K	Rajesh K	• Updated Business Response Team for delivery. • Updated Pramati Chennai office address. • Updated contact details of Finance manager.
5.0	9-Feb-2018	Rajesh K	Rajesh K	ISF	Updated BCP Contacts under the section “3.0 Appendix.”

Contents

1.0 Introduction

1.1 Overview

Business continuity planning is critical requirements due to fact that regular business activities might get disrupted due to unforeseen events. Preventive and disaster recovery mechanisms are planned, budgeted, documented and implemented formally to face such situations.

1.2 Purpose

The purpose of this document is to ensure that the procedures and responsibilities are planned to ensure business continuity and resume business critical activities in a planned way in case of a disaster. The basis of this plan is the business impact analysis carried out with each of the business function and business unit within the organization and also on the basis of the assessment of the contractual obligations if any in this regard.

1.3 Target Audience

This document is referred by all business functions and business units to apply necessary controls for business continuities.

1.4 Acronyms / Definitions

Acronym/ Definition	Description
BCP	Business continuity plan
DR	Disaster recovery
COO	Chief Operating Officer
CISO	Chief Information Security Officer
VP	Vice President
CFO	Chief Financial Officer
ERT	Emergency Response Team

1.5 Roles

- Business Response Team
- ISO
- Executive Management
- Senior Management

1.6 References

- ISO 27001:2013
- ISMS Manual
- Business continuity management process
- Business Impact Analysis Matrix

2.0 Operating Process

2.1 Business Continuity Strategies

Please document business continuity strategies along with their rationale.

Area	BC Strategy	Business Function/Unit	Rationale
Disaster recovery (DR)- Physical office backup facility	City Outage: Pramati's Chennai office is identified as the DR location for Hyderabad location. The same applies for Chennai and Bangalore locations Local Disruption: Team members can work from home	Pramati's Chennai office has a 180 seater capacity that can act as a backup for ensuring critical projects and functions are up and running if need be.	Chennai being another location of Pramati has been identified as the DR location and the facility is kept 24x7 ready to face any eventuality. Bangalore is another alternate DR location which operates on 24x7.
Offsite data backup	Critical information pertaining to Finance, HR, Admin, IT support, our product IP, Key laptops and data of Imaginea's delivery heads, engagement managers are considered to be separately backed up apart from the physical back up that is currently in place. Offsite data backup currently pursued is expected to be on the cloud.	Covers all the functions, heads and key personnel along with our own product IP.	Ensure we are still able to backup critical information if something happens to the physical, periodic backup that happens on the NAS drive and stored in a fire-proof safe.
Automated Backup and restoration plan under IT team's purview	Currently all the major information assets related to finance, HR, admin, IT support and delivery, our products' IP (SocialTwist,) few critical customer specific project's related source code, along with important artifacts that the project leaders choose are backed up on a defined weekly, monthly and incremental day backup modes in our pacific server in the Midtown office. Important data on the	Covers all the functions, heads and key personnel along with our own product IP.	Systematic backup procedure for ensuring appropriate business continuity management to be in place.

Area	BC Strategy	Business Function/Unit	Rationale
	pacific server also gets backed up with a 3 year archival mechanism. The IT teams use a backup tool to perform a scheduled, automated and reported backup. Apart from this, on need basis, every Pramati resource is provided a personal folder on the pacific server that can be used for the individual's preferred backup.		
Electricity and Power backup	All the major facilities (i.e., Hyderabad, Bengaluru and Chennai centers) have been adequately backed up with electricity and power backup systems. Measures are defined and in place to have critical servers up and running instantly with online UPS from the time of power shutdown. Scheduled maintenance is performed to ensure constant overhaul of the generators and the UPS backup.	Covers all the work force spread across these three facilities.	Ensure business continuity happens with a very low or no downtime for all frontline deliveries ensuring customer confidence is maintained always.
Internet and bandwidth backup	Our IT support team ensures they have a critical SLA defined with our ISP assuring up to 99% of availability. We have an adequate back up of Internet infrastructure.	Covers all the work force spread across these 3 facilities.	Ensure business continuity happens with a very low or no downtime for all frontline deliveries ensuring customer confidence is maintained always.
SLAs with all the external party agreements	SLAs and guarantee agreements/ docs with all the external party vendors ensure we receive the best in class, on time services from respective vendors/	Covers all the work force spread across these 3 facilities.	Ensure business continuity happens with a very low or no downtime for all frontline deliveries ensuring customer confidence is maintained always

2.2 Roles and Responsibilities

Roles	Responsibilities
BCP Head	Coordinate with Department Heads. Assesses disaster situation and execute necessary action.
Functional Heads	Allocate resources for implementation and testing.
BCP Team	Coordinate BCP activities.
ERT	Ensures Safety of People.

2.3 Conditions for the Activation of Plan

Business Continuity Plan is expected to be operational for testing and maintenance.

Critical Function / Service Name	Conditions for Activation of the Plan
- Delivery	Facility inaccessible for more than one business day People unable to operate at 80%
- Citrix Admin and Support	Facility inaccessible for more than one business day People unable to operate at 80%
- Network Admin and Support	Facility inaccessible for more than one business day People unable to operate at 80%
- Facility Management	Facility inaccessible for more than one business day People unable to operate at 80%

2.3.1 Activities Performed

2.3.1.1 Define Business Continuity & Disaster recovery Plan

Activities	Resp.
Identify critical processes	BCP Head
Estimate loss due to loss of critical services due to disaster	BCP Head
Evaluate BCP requirements for critical business processes	BCP Head
Review and approve critical processes business continuity requirements	ISMS Team Head Operations
Identify the client specific BCP requirements	ISMS Team
Capture business continuity requirements while gathering IT Infrastructure requirements	BCP Head
Include any need for business continuity arrangements explicitly required in contractual requirements	BCP Head

Activities	Resp.
Carry out the Business Impact Analysis for each function	ISMS Team
Review Business Impact Analysis Results	BCP Head
Map related information assets of Critical Processes	BCP Head
Identify the Natural, Man-made and Technical disaster associated with Assets	BCP Head
Check identified Critical Process Assets are covered as part of Risk Assessment Process	BCP Head
If covered in Risk Assessment, Check adequacy of risk mitigation for asset	BCP Head
Document Disaster Recovery Process for Critical Key Process	BCP Head
Establish Disaster Recovery Plan for Asset of Critical Key Process	BCP Head
Consolidate entire Disaster Recovery Plan for identified Critical key process	BCP Head
Recover Facilities	Admin
Recover Facilities services	Admin
Inform Vendors for Support, if required	Admin/IT
Restore Servers	IT
Restore Networks	IT
Assets if the operations have returned to normalcy	BCP Head
Inform employees about Normal Operations	ERT
Inform Clients about Normal Operations	ERT
Analyze Disaster Recovery Effectiveness	BCP Head
Identify improvements in Disaster Recovery Process	ERT

2.3.1.2 Implement Business Continuity & Disaster recovery Plan

Activities	Resp.
Assign roles and responsibilities for BCP Implementation	BCP Head
Communicate roles and responsibilities for BCP Implementation	BCP Head

Activities	Resp.
Ensure availability of necessary resources for BCP Implementation	ISMS Team
Implement measures identified in BCP	BCP Team
Carry out Client Specific BCP, if any	BCP Team
Monitor execution of BCP	BCP Head
Take corrective action to ensure smooth implementation of BCP	BCP Head
Update the BCP periodically or when there is a change in the business environment	BCP Head
Inform Clients about Disaster	Head Operations
Inform Other Facilities	BCP Head
Inform critical vendors if necessary	Admin/IT
Arrange for transport to shift to alternate location	Admin
Inform staff at alternate location to release capacity if necessary	Head Operations
Arrange necessary requirements for extended work hours (food, water, medicines, extended housekeeping services, beds etc.)	Admin
Recover essential Facilities	Admin/ISMS
Recover essential Facilities services	Admin
Activate DR Site if necessary	IT
Inform Vendors for Support, if required	IT
Restore Essential Servers	IT
Restore Essential Networks	IT
Restore Work Stations	IT

2.3.1.3 Develop Business Continuity Test Plan

Activities	Resp.
Develop BCP test plan	BCP Head/CISO
Document all assumptions and constraints for BCP Testing	BCP Head
Develop specific test plans based on various scenarios	BCP Team

Activities	Resp.
Select type of BCP test	BCP Team
Review BCP test plan	ISMS Team
Validate assumptions and constraints	ISMS Team
Prepare necessary checklist for BCP Testing	ISMS Team
Conduct test as per BCP test plan	BCP Team
Monitor BCP Testing	BCP Head
Document test results	BCP Team
Review BCP Test result	ISMS Team
Update BCP based on audit results	BCP Head

2.3.1.4 Improve Business Continuity Process

Activities	Resp.
Analyze Business Continuity Process Effectiveness	BCP Head

2.4 Business Continuity Scenarios

2.4.1 Non availability of facility

2.4.1.1 Condition to activate the plan

Facility is not available due to fire.

2.4.1.2 Emergency Phase

- Inform Head-Admin or Security Personnel.
- Fire wardens/Security Personnel/ Electricians can tackle small fires by using the fire extinguishers kept at the prominent location inside the facility, Electrical room, UPS room and DG set area when it is in the incipient stage, (without endangering themselves) however keep fire brigade informed right in the beginning. Refer Appendix C for list of fire wardens
- In case of any major fire accidents do not take risk, hand over the site to fire brigade.
- When you summon the fire brigade, mention Your Name, Address, Telephone Number, Important Landmarks, and Type of Fire. Note down the time of calling
- Shut off the power supply to the affected area. If required maintain domestic lighting.
- Electricians to put off all the air-conditioning. Ground all the elevators and switch-off. Do not use elevators.
- On fire brigades arrival give total assistance; give clear information about the affected block/ facility. Show them the water facility available in the site. Keep all the onlookers out & help the security. Keep all the vehicles out of the complex at safe distance. Salvage the

un-burnt materials around the accident spot.

2.4.1.3 Evacuation Guidelines

- Position yourself at a convenient place in your designated floor or move around, be alert.
- Direct all the occupants to appropriate and nearby exit. Do not use lifts/elevators (ground the lift and switch it off)
- Help to evacuate physically challenged, women and all the rest of the employees through the emergency exits/staircase
- Make way on one side of the staircase for fire brigade personnel to come up and help
- Check restrooms, Storage rooms & Conference rooms.
- Keep repeating “Take a brisk walk and don’t run” – through announcements by fire wardens
- While evacuating occupants from smoke filled areas advise the occupants to crawl on their hands and knees below the smoke level, if necessary instruct them to tie wet kerchief across nose and mouth. This prevents the entry of smoke/toxic gases.
- Once the total evacuation gets over in your designated floor, rush to the safe assembly point and report to fire wardens
- Fire wardens to check the head counts/attendance rolls (including those of the visitors) at the assembly point at facility.
- Once taking the head count/ attendance let the people go outside the premises.
- If anyone is missing, help fire brigade in search operations
- Do not allow anybody to re-enter the facility till all-clear signal is given by fire wardens.

2.4.1.4 First Aid

- A First-Aid box is kept available in the reception area & security desks to facilitate employees to use it in case of emergency.
- First Aid is by definition the immediate care given to the injured or suddenly ill person. First aid does not take the place of proper medical treatment. It consists only of giving temporary assistance until competent medical care is obtained or until the chance for recovery without medical care is ensured.
- Any trained First-Aid person can give the First Aid
- Do not attempt when you are in doubt-remember you could do more damage than help the victim.
- Use the First Aid Box prominently displayed.

Reference: First Aid Guidelines (V 1.0)

2.4.1.5 Backup phase

- In cases where there is partial damage to the facility, safety and security of working in undamaged portion of the damaged site after securing necessary regulatory approvals shall be ensured.
- Inform customers about the revised service levels/ delivery commitments during the back-up phase.

2.4.1.6 Resumption phase

- Assess damage. Inform Insurance Agency with details regarding the incident.
- Discuss with Service providers and Vendors. Estimate the time required to bring the site back to normal.
- If bringing back the site back to normal is not feasible within reasonable time meeting contractual agreements/ service levels with the customer the same will be discussed with

customer

- Get necessary budget approvals. Lay down a task plan to get the site back to normal.
- Resume full operations in a phased manner.

2.4.1.7 Business Response Team

- Sampath K, Somnath D, Syed K, Dinesh K – Admin and Operations, Pramati, Hyderabad, Bangalore & Chennai
- Shruthi S, Dimple P, Aarthy S - HR, Pramati, Hyderabad , Bangalore & Chennai
- Prashanth J, Ravi G, Syed Z and Dinesh K – IT Team, Pramati, Hyderabad, Bangalore and Chennai.
- Dominic G, Srikumar S, Arghya Chaudhuri – Delivery Heads
- Rajesh Kumar – CISO
- Chetan L, Anitha P – Human Resources
- Harish T- Finance
- Chandrasekhar Sivaraman, Giri Kuthethoor and KV Prasad – Sr, Management
- BRT Team for Fire Alarms- A separate BRT team for fire alarms and fire contingencies under the leadership of Sampath is place

2.4.1.8 Recovery Team

All the function Heads.

2.4.1.9 Test approach

- Simulate as if fire incident has occurred at the site.
- Fire wardens help the employees with evacuation.
- Observe, understand and document the learning. Where required, make changes to the BCP accordingly.
- The frequency of mock fire drill takes place on a yearly basis.

2.4.2 Failure of Communication Services

2.4.2.1 Condition to activate the plan

When communications such as internet or telecommunications fail and restoration time is beyond the service levels.

2.4.2.2 Emergency Phase

- Inform Senior Management
- Inform other facilities /clients where necessary (and whoever gets impacted due to the failure)

2.4.2.3 Backup phase:

- Till restoration of failed communication, traffic will be diverted through alternate path.
- Inform all about the reduced performance and service levels.
- Inform all about the new interim communication arrangements.

2.4.2.4 Resumption phase

- Inform the service provider
- Coordinate with servicing agency for immediate resumption of the service

- Test the service once it comes up. Confirm service is stable
- Provide connectivity and inform the customers.

2.4.2.5 Business Response Team

- Appropriate BRT is in place.

2.4.2.6 Recovery Team

- Members of IT Support and Admin Team

2.4.2.7 Test approach

- Mock testing by making the communication service down for a defined period and keep all the stake holders, clients and risk owners informed about the drill well in advance.

2.4.3 Failure of critical IT Infrastructure

2.4.3.1 Condition to activate the plan

- Confirmed electrical supply including connections are ok and Server is not coming up after trying to reboot twice and Server is down for more than 20 minutes

2.4.3.2 Emergency Phase

- Inform Senior Management

2.4.3.3 Back-up Phase

Server Name	Alternate equipment Identified	Procedure to install/activate Backup Server	Estimated Time
Pacific	NAS drive	Retrieval of the lost information on the pacific server is done by the IT team. They have a trained and well established, automated mechanism to retrieve information, data from the NAS drive.	<=4 hours
Local desktops, mail server, active directory and product IP of Socialtwist Pramati server	Pacific	Using the backup tool with an automated procedure	<= 4 hours
www.pramati.com, www.imaginea.com, www.socialtwist.com	Amazon S3 buckets	Amazon standard procedures	<=1 hour

Production servers of Social Twist	Amazon S3 buckets	Amazon standard procedures	Archival is not applicable for Social Twist. Only last 3 good backups are maintained and all other backups are deleted.
Database content servers of Socialtwist	Amazon S3 buckets	Amazon standard procedures	Archival is not applicable for Social Twist. Only last 3 good backups are maintained and all other backups are deleted.

2.4.3.4 Resumption Phase

- The IT Support personnel inform the concerned service providers and affected group.
- Coordinate with servicing agency for replacement
- Get the replacement server installed / Restoration of the backup
- Ensure proper security policy in the server
- Test the replacement server
- Change over to the replacement server from spare server
- Restore relevant data to the replacement server
- Update Asset/ Server details with respect to new server
- Make sure that electronic media does not contain critical information assets, if the server is taken up by the maintenance service provider
- Inform affected groups on the resumption of service with new / updated server.

2.4.4 Failure of Critical Communication & Networking Equipment

2.4.4.1 Emergency Phase

- Inform IT Support Personnel and Delivery Heads

2.4.4.2 Back-up phase

Communication Equipment/ Connectivity	Alternate equipment identified	Procedure to activate Backup Equipment	Estimated Time
ISP	Alternate/ Backup service provider identified and in place.	Automatic switch over.	<=0.5 hours

VoIP and communication infrastructure	Alternate lines and backup in place	Automatic switch over.	<=0.5 hours

2.4.4.3 Resumption Phase

- Inform service providers and affected customers
- Coordinate with servicing agency & vendor for replacement.
- Get the replacement device and change over to the replacement device from spare device.
- Inform affected groups on the resumption of services.

2.4.4.4 Business Response Team

- Sampath K, Somnath D, Syed K, Dinesh K – Admin and Operations, Pramati, Hyderabad , Bangalore & Chennai
- Shruthi S, Dimple P, Aarthy S - HR, Pramati, Hyderabad , Bangalore & Chennai
- Prashanth J, Ravi G, Syed Z and Dinesh K – IT Team, Pramati, Hyderabad, Bangalore and Chennai.
- Rajesh Kumar – CISO
- Dominic G, Srikumar S, Arghya Chaudhuri – Delivery Heads
- Chetan L, Anitha P – Human resources
- Harish T- Finance
- Chandrasekhar Sivaraman, Giri Kuthethoor and KV Prasad – Sr, Management
- BRT Team for Fire Alarms- A separate BRT team for fire alarms and fire contingencies under the leadership of Sampath is in place

2.4.4.5 Recovery Team

- Prashanth J, Ravi G, Syed Z and Dinesh K – IT Team, Pramati, Hyderabad, Bangalore and Chennai.

2.4.4.6 Test approach

- Mock testing with making the service down

2.4.5 Computer Virus Outbreak

2.4.5.1 Emergency Phase

- Inform the Senior management and functional heads

2.4.5.2 Back-up Phase

- NA

2.4.5.3 Resumption phase

- Identify the infected computer
- Disconnect the computer from Network
- Scan the computer thoroughly through antivirus
- If required scan the computer and reinstall software
- Check for the normal functioning of the computer
- Connect the computer in LAN

2.4.5.4 Business Response Team

- Sampath K, Somnath D, Syed K, Dinesh K – Admin and Operations, Pramati, Hyderabad ,

Bangalore & Chennai

- Shruthi S, Dimple P, Aarthy S - HR, Pramati, Hyderabad , Bangalore & Chennai
- Prashanth J, Ravi G, Syed Z and Dinesh K – IT Team, Pramati, Hyderabad, Bangalore and Chennai.
- Rajesh Kumar – CISO
- Dominic G, Srikumar S, Arghya Chaudhuri – Delivery Heads
- Chetan L, Anitha P – Human resources
- Harish T- Finance
- Chandrasekhar Sivaraman, Giri Kuthethoor and KV Prasad – Sr, Management

2.4.5.5 Recovery Team

- Members - IT Teams, Pramati, Hyderabad, Bangalore and Chennai.

2.4.6 Failure of Power critical Equipment

2.4.6.1 Emergency Phase

- Inform the senior management and function heads
- Inform to Power Distribution Office for early restoration of power
- Inform to other service providers (UPS and DG sets).

Please refer Section 3.2 for contact details of Group Heads

2.4.6.2 Back-up Phase

- As UPS, DG sets are operating 1+1 Backup auto swap is being adopted for alternate source of supply.
- If redundancy arrangements failed, based on the severity of problem, plan for alternate arrangements.
- Contact the service providers to report at the site for back-up arrangements.
- Make stand-by arrangements
- Hire the equipment (UPS systems, DG sets, etc.), if required and deploy

2.4.6.3 Resumption phase

- Coordinate with servicing agency for immediate resumption of the service
- After restoration of power, test the service once
- Swap all the equipment to the old setup
- Inform all the concerned. Inform the service provider
- Confirm service is stable
- Provide connectivity and inform the users.

2.4.6.4 Business Response Team

- Sampath K, Somnath D, Syed K, Dinesh K – Admin and Operations, Pramati, Hyderabad , Bangalore & Chennai
- Shruthi S, Dimple P, Aarthy S - HR, Pramati, Hyderabad , Bangalore & Chennai
- Prashanth J, Ravi G, Syed Z and Dinesh K – IT Team, Pramati, Hyderabad, Bangalore and Chennai.
- Rajesh Kumar – CISO
- Dominic G,Srikumar S, Arghya Chaudhuri – Delivery Heads
- Chetan L, Anitha P – Human resources
- Harish T- Finance

- Chandrasekhar Sivaraman, Giri Kuthethoor and KV Prasad – Sr, Management
- BRT Team for Fire Alarms- A separate BRT team for fire alarms and fire contingencies under the leadership of Sampath is in place

2.4.6.5 Recovery Team

- Members – Admin and Facilities Team, IT Team, Department Heads.

Roles are already defined above and the names may be appended in the “Information Security Organization” document against each role.

2.4.7 Medical Emergency

2.4.7.1 Emergency Phase

- Immediately call for rescue squad or ambulance.
- To insure adequate breathing, open and maintain the victim's airway by gently tilting head back. If victim is NOT breathing, immediately begin mouth-to-mouth resuscitation.
- Check and periodically recheck the victim's carotid pulse in the neck, using two fingers. If pulse is not present, immediately begin CPR.
- Stop all obvious bleeding by applying direct pressure over the wound with your hand. If available, use a clean cloth or bandage.
- Do not move victim unless a hazard is present. Keep the victim in a quiet, comfortable position.
- Loosen all tight clothing.
- Keep victim warm - do not induce sweating.
- Give no fluids - except very small sips of water, only if requested by the victim.
- Elevate victim's legs slightly, unless an injury is present on the chest or head.
- Comfort and reassure the victim constantly.
- For all on-the-job injuries, notify your supervisor as soon as possible.
- Reduce unnecessary employee traffic around the area

2.4.7.2 Backup Phase

- NA

2.4.7.3 Resumption Phase

- Take note of specifics (who was involved, what happened, when did it occur, where did it occur).
- Discuss with concerned delivery head over identified back up resource for delivery to be seamless.

2.4.7.4 Business Response Team

- Sampath K, Somnath D, Syed K, Dinesh K – Admin and Operations, Pramati, Hyderabad , Bangalore & Chennai
- Shruthi S, Dimple P, Aarthy S - HR, Pramati, Hyderabad , Bangalore & Chennai
- Prashanth J, Ravi G, Syed Z and Dinesh K – IT Team, Pramati, Hyderabad, Bangalore and Chennai.
- Rajesh Kumar – CISO
- Dominic G Srikumar S, Arghya Chaudhuri – Delivery Heads
- Chetan L, Anitha P – Human resources

- Harish T- Finance
- Chandrasekhar Sivaraman, Giri Kuthethoor and KV Prasad – Sr, Management

2.4.7.5 Recovery Team

- Members - Emergency Response Team, IT team, HR and Admin teams.
- Confirm with HR and Admin about the employee being taken to hospital
- If required, assist HR/Admin to talk to hospital over insurance and employee details
- Reach out to family concerned, team lead and delivery head
  Reference: First Aid Guidelines (V 1.0)

2.5 Technology Availability Plan

S.No.	Technology Resource / Component	Description	Scenario	Impact	Recovery Priority	Business Continuity Plan
1	Network	MPLS connectivity	MPLS outage	Very High	Very High	Switch over to the Internet line
2	Network	Internet connectivity	Internet outage	Very High	Very High	Continue to use MPLS as the primary link
3	Network	MPLS & Internet connectivity	MPLS & Internet outage	Very High	Very High	Critical resources across all verticals will use their respective data cards for both data and phone accessibility.
4	IT Infrastructure	Server infrastructure	Server hardware outage causing unavailability of AV updates.	High	High	N.A

2.6 Disaster Scenario Analysis Plan

This section contains different scenarios for disasters and mitigation and resource planning for the same.

	Scenario 1	Scenario 2	Scenario 3 - A	Scenario 3 -B	Scenario 4	Scenario 5	Scenario 6	Scenario 7	Scenario 8
People	Available	Available	Available	Available	Available	Not Available	Not Available	Not available	Not Available
Facility	Available	Available	Not Available - Unplanned	Not Available - Planned	Not Available	Available	Not Available	Available	Not Available
IT Infra	Available	Not Available	Available	Available	Not Available	Available	Available	Not available	Not Available
Common Scenarios		HW Failure Virus Attack Network Outage Power Outage AC Outage	Damages to facility due to Natural Elements/ Man-made elements (harsh weather conditions, terrorist activities, bombs etc.)	Facility not accessible due to Bandh / Riots etc.	Will be covered as Scenario 2 and 3	Strike Pandemic Mass exit/resignation Key people unavailability Food poisoning	Remote probability	Covered as part of scenario 5 & 6	Damages to facility due to Natural Elements / Man-made elements Covered as part of scenario 5 & 6
Likelihood	High	Medium	Medium	Medium	Medium	Medium	Medium	Low	Low
Impact	Low	High	High	Medium	High	High	High	High	High
Contingency Plan	Business as usual	Work from home based on approval	Work from home based on approval	Work from home based on approval	Work from home based on approval	On-site functional managers and team from other location to take	People from other location to take over	People from other location to take over	People from other location to take over

	Scenario 1	Scenario 2	Scenario 3 - A	Scenario 3 -B	Scenario 4	Scenario 5	Scenario 6	Scenario 7	Scenario 8
						over			
Group Responsible	BCP Team	Infra	Admin/Operations	Operations/ Admin / IT	IT and Admin	Operations / HR	Operations/ HR / Admin	Business Continuity Management Team	Business Continuity Management Team
Pre-requisites to make the plan successful	Not applicable	Backup and alternate arrangements for redundant link	Alternate location with additional capacity Transport PC and data card / broadband	Laptop and data card	Laptop and data card	People in other location should be equipped to takeover with respect to processes and policies	People in other location should be equipped to takeover with respect to processes and policies	People in other location should be equipped to takeover with respect to processes and policies	People in other location should be equipped to takeover with respect to processes and policies
Current Mitigation Plan	Not applicable	Broadband / Blackberry connection provided to identified resources to work from remote location	Resources available for carrying out shifts will be communicated to work from remote location	Resources available for carrying out shifts will be communicated to work from remote location	Resources available will be moved to alternate work location (Head-office at Hydera	People operating in present time frame at work location will be continuing operations	People operating in present time frame at work location will be equipped with internet broadband through	People operating in present time frame at work location will be equipped with internet broadband through data	Process owners in other geographic location will take over operations at Pramati Technologies Bangalore

	Scenario 1	Scenario 2	Scenario 3 - A	Scenario 3 -B	Scenario 4	Scenario 5	Scenario 6	Scenario 7	Scenario 8
					bad)		h data card	card	
Possible Additional Mitigations	Not applicable	To be planned on need basis	To be planned on need basis	To be planned on need basis	To be planned on need basis	To be planned on need basis	To be planned on need basis		

2.7 BCP Test Plan

Aspect to be tested	Frequency	Responsibility	Remarks
Network/ISP redundancy test	Annually	IT	
Facility availability	Annually	Admin	
UPS Test/Power Backup	Annually	Admin	
Fire extinguisher check	Annually	Admin	
Fire Evacuation	Annually	Admin	

3.0 Appendix

3.1 Alternative Site Information

- **Pramati Technologies - Chennai Development Center**

  114, Rajiv Gandhi IT Expy, Phase-2,
  Thirumalai Nagar Annexe,
  Perungudi,
  Chennai, Tamil Nadu 600096
  Phone: 044 3355 2000

- **Pramati Technologies – Bangalore Development Center**

  15th Floor, Brigade World Trade Centre
  26/1, Dr.Raj Kumar Road, Malleswaram West
  Bangalore, Karnataka 560 055
  Phone: 080 4960 9999

- **Pramati Technologies**

  Mid Town 6-3-348,
  Road No. 1,
  Banjara Hills,
  Hyderabad, Telangana 500034
  Phone: 040 3355 2000

3.2 Contact Details of Department & Group Heads

S No	Name & Role	Department / Group	Contact Number	Email ID
1	KV Prasad - COO	Imaginea	9849090130	kvp@imaginea.com
2	Chandrasekhar Sivaram – SVP + ISO and Head Chennai Dev Center	Imaginea	9003074413	chandru@pramati.com
3	Harish T – CFO	Pramati	9849201205	harish@pramati.com
4	Giri Kuthethoor – SVP + ISO and Head, Bangalore	Imaginea	9731177992	Giri.k@imaginea.com
5	Chetan I Shinde – SVP, HR	Pramati	9880042260	Chetan.I@pramati.com
6	Kalyan Ram Kuppachi - VP, Customer Success	Pramati	9885158028	kalyan.kuppachi@imaginea.com
7	Sampath Lakshmi Narsimhan – Director, Admin	Pramati	9052901235	sampath.kumar@pramati.com
8	Rajesh Kumar –CISO	Imaginea	9916698169	rajesh.kumar@imaginea.com
9	Anitha Prabhakar-	Pramati	9989396086	Anitha.prabhakar@pramati.c

	Director, HR			om
10	Prashanth Jala- Director, IT	Pramati	9849034995	Prashanth.jala@pramati.com
11	Dominic George – Director, Engineering	Imaginea	8297038786	dominic.george@imaginea.com

3.3 Hyderabad Contact Numbers

INTERNAL EMERGENCY CONTACT NUMBERS			
Response person	**Department / Designation**	**Extension**	**Mobile #**
Security	Reception -Security	8004	8004
Deepshikha Saxena	Executive - Front Office	5	9618277600
B.Srinivas	Facilities-AM	7529	9885309974
Somnath Danda	Sr.Manager Admin	14056	9618899984
Sampath Kumar	Director Facilities & Admin	14016	9052901235
Satish Kumar.V	Asst Manager-Finance	14051	9848278491
IT-Support	IT-Support	8888	8888
Ravi Gokara	IT-Manager	14054	9618926555
Prashanth Jala	Director - IT	14006	9849034995
Anitha Prabhakar	Director - HR	14013	9989396086

EXTERNAL EMERGENCY CONTACT NUMBERS				
Location	**Response person**	**Designation**	**Land Line #**	**Mobile #**
Police Stations-108/100				
Panjagutta	Nagaiah	Inspector	040-27852494	9618398031
Panjagutta	Sattaiah Yadav	Detective Inspector	040-27852019	9490616613
Panjagutta	S. Mohan Kumar	SHO	040-23852019	9490616610
Jubilee Hills	S.Venkat Reddy	SHO	040-27852447	9490616585
Fire Stations-108/101				
Film Nagar	D.Mohan Rao	Fire officer	040-23442953	9441847966

Secretariat	K.Mohan	Station In Charge	040-23442947	9963737540/ 9346795773
	K.Vijay Kumar	Fire Officer		9346368667/ 8897508937
Sanathnagar	M.A.Sharif	Fire Officer	040-23442946	9393188437
Medical Emergency-108/102				
Banjara Hills	Care Hospital		040-30418888 / 66668888	
Somajiguda	Yashoda Hospital		040-23319999	
Secunderabad	Yashoda Hospital		040-67778999	
Jubilee Hills	Apollo Hospital		0040-23607777	
Blood Bank				
Banjara Hills	Care Hospital		040-30417777	
Jubilee Hills	Chiranjeevi Blood Bank		040-23559555	
Vidyanagar	Red cross Blood Bank		4027633087	
Electricity Emergency				
Control Room			040-23235305	
Banjara Hills	Madhu	A.E		9440812860
Banjara Hills	Raju	Linemen		9391309684

3.4 Bangalore Contact Numbers

Names		Mobile	Desk Phone
Ajith Kumar		8884666196	080 49069803
Ameet Kumar Patnaik		9886772870	6306473040
Arun Krishnamurthy		9902763372	6306473059
Arun Mariappan		9008733448	6306473027
Diwakar Chaudhary		9108288957	6306473013
Gaurav Singh		7829820431	6306473040
Jenifer Pattudurai		9900225343	6306473086
Manjul Abhishek		9035149782	6306473026
Pavan Nayak		8861584052	6306473141
Prasanna Kumar		9620968777	080 49069802
Prasanta Kumar Lenka		9886806444	6306473009
Praveen Gururao		9900117775	6306473067
Preetham Sunil		9742568669	6306473063
Ranjan Kakade		9844916910	6306473058
Shobha Chandrashekara		9845918095	080

			49069805
Srivatsan Parthasarathy		9901544994	6306473027
Stany Pinto		9740068968	6306473039
Syed Kadhar		9880108739	080 49069806
Syamini Sreedharan		9746997735	6306473031
Syed Zabiulla		9845393217	6306473030
Vivek Kasiperumal		9980364531	6306473001
Arun Kumar		9739651469	6306473088
Gangadhar	Security Guard	9845920470	080 49069999
Hanumesh	Security Supervisor	9880820585	080 49069999
Kariyappa	Security Guard	9740645096	080 49069999
Kumar	Security Supervisor	8970938707	080 49069999
Siddaraju	Security Guard	8088094211	080 49069999
Siddegowda	HK Supervisor	9844329645	080 49069999
Vijaya Kumar	Security Supervisor	7795665165	080 49069999
Pramati Reception			080 49069999
WTC			
WTC Helpdesk			080 49019000
Police Station			
Police Control Room			100
Subramanya Nagara Police Station		080 22942524	080 23322422
Rajajinagar Police Station		080 22942522	080 23324647
Yeshwanthpur Police Station		080 22942526	080 23346472
Fire Station			
Fire			101
Central Fire Station		080 22971500	080 22971600
Rajajinagar		080 22971543	
Yeshwanthpur		080 22971544	
Hospitals			
Columbia Asia Yeshwanthpur		080 39898969/91	080 30115555

Fortis		080 23014444	
ESI Rajajinagar		08023324112/1233	
Ambulance		102	108

3.5 Chennai Contact Numbers

EXTERNAL EMERGENCY CONTACT NUMBERS			
Police Station	Ambulance	Apollo Hospital,Perungudi	Fire station
100	108	044 - 24961111	044 - 24401213
		044 - 28291066	044 - 22435043
Department	**Contact Person**	**Mobile**	**Desk**
Engineering	Chandrasekhar Sivaraman	9003074413	23551
	Senthil Jayabalan	9840279921	23561
	Sita Krishnakumar	9003070867	23578
	Srikumar.S	9442090229	23573
Admin	Aravinth	8939902040	23576
IT	Dinesh Kumar	9840744887	23555
HR	Aarthy	9884332396	23577
Board Number	Security / Front Office	044-33552000	23599
Security	Tapan Kumar Nayak	7338942097	
	Mohanty	9884946833	
Electrician	Muniprakash	9944082226	
	Neelagandan (Origin)	9840862176	

3.6 Insurance and Finance Companies

Location	Service	Company	Telephone
Hyderabad	Banking	CITI Bank	Soumen Kundu @ +918801764134
Hyderabad	Insurance	United India Insurance	Hareesh Patrudu L @ 8019321988 Email: hareeshl@uiic.co.in
Hyderabad	Insurance	Prudent Insurance	JoyDip Bhattacharjee 9000810301 / 8008588850 joydip.b@prudentbrokers.com
Bangalore	Banking	ICICI Bank	Raju 7899747360
Bangalore	Insurance	Futurisk	Indu – 9972822003 9632943002

Chennai	Banking	CITI Bank	Piyush - 7299130521
Chennai	Insurance	Mediassist	Dharmendra - 9551096465