

Section I: Introduction

A. How to Use This Plan

In the event of a disaster which interferes with Cellcomm company's operation and business activities, this plan is to be used by the responsible individuals to coordinate the recovery of their respective areas. The plan is designed to contain, or provide reference to, all of the information that might be needed at the time of a recovery.

This plan is not intended to cover the operations of Cellcomm's separately structured Team (Crisis Management Team).

Index of Acronyms: (BCP) Business Continuity Plan; (IT) Information Technology

Section I, Introduction, contains general statements about the organization of the plan. It also establishes responsibilities for the testing (exercising), training, and maintenance activities that are necessary to guarantee the ongoing viability of the plan.

Section II, Business Continuity Plan, describes the strategy that the Crisis Management Team will control/implement to maintain business continuity in the event of company's operation and business activities disruption. These decisions determine the content of the action plans, and if they change at any time, the plans should be changed accordingly.

Section III, Recovery Teams, lists the Recovery Team functions, those individuals who are assigned specific responsibilities, and procedures on how each of the team members is to be notified.

Section IV, Team Procedures, determines what activities and tasks are to be taken, in what order, and by whom in order to affect the recovery.

Section V, Appendices, contains all of the other information needed to carry out the plan. Other sections refer the reader to one or more Appendices to locate the information needed to carry out the Team Procedures steps.

B. Objectives

The objective of the Business Continuity Plan (BCP) is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services.

The priorities in a disaster situation are to:

1. Ensure the safety of employees and visitors in the office buildings.
2. Mitigate threats or limit the damage that threats can cause.
3. Have advanced preparations to ensure that critical business functions can continue.
4. Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.

The Cellcomm Centre BCP includes procedures for all phases of recovery as defined in the Business Continuity Plan section of this document.

Appendix A – Categorization of Disaster Events & Impact

C. Scope

The Business Continuity Plan is limited in scope to recovery and business continuance from a serious disruption in activities due to non-availability of Cellcomm company's operation and business activities. The Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Plan of this document. This plan focuses on the recovery of facilities and platforms, company's operation and business activities. Unless otherwise modified, this plan does not address temporary

interruptions of duration less than the time frames determined to be critical to business operations.

The business continuity plan:

- realistically formalises the actions Department will need to take
- minimises the downtime for the business
- Identifies business priorities so that if services are limited, they can be allocated effectively.

The scope of this plan is focused on localized disasters such as fires, floods, and other localized natural or man-made disasters. This plan is not intended to cover major regional or national disasters such as regional earthquakes, war, or nuclear holocaust. However, it can provide some guidance in the event of such a large-scale disaster.

D. Changes to the Plan/Maintenance Responsibilities

Maintenance of the Cellcomm company's operation and business activities BCP is the responsibility of the Crisis Management Team.

Crisis Management Team is responsible for:

1. Periodically reviewing the adequacy and appropriateness of its Business Continuity Plan.
2. Assessing the impact on the Cellcomm centre BCP of additions or changes to existing business functions, Department. procedures, equipment, and facilities requirements.
3. Keeping recovery team personnel assignments current, taking into account promotions, transfers, and terminations.
4. Plan Testing Procedures and Responsibilities

Crisis Management Team are responsible for ensuring the workability of their Business Continuity Plan. This should be periodically verified by active or passive testing.

E. Plan Training Procedures and Responsibilities

Crisis Management Team are responsible for ensuring that the personnel who would carry out the BCP are sufficiently aware of the plan's details. This may be accomplished in a number of ways including; practice exercises, participation in tests, and awareness programs.

Section II: Business Continuity Plan

A. Introduction

BCP describes the strategy devised to maintain business continuity in the event of a disruption. This strategy would be invoked should company's operation and business activities somehow be disrupted, damaged or inaccessible.

B. Business Function Recovery Priorities

The strategy is to recover critical company's operation and business activities. Information Systems will recover based on the critical business functions and defined strategies.

Business Functions those of which are of the most critical for immediate recovery are:

Reference: Appendix B – Recovery Priorities for Business Functions

C. Recovery Plan Phases

The activities necessary to recover from company's operation and business activities disaster or disruption will be divided into three (03) phases. These phases will follow each other sequentially in time.

1. Disaster Occurrence

This phase begins with the occurrence of the disaster event and continues until a decision is made to activate the recovery plans. The major activities that take place in this phase includes: **emergency response measures, notification of management, damage assessment activities, and declaration of the disaster.**

2. Plan Activation

In this phase, the Business Continuity Plans are put into effect. This phase continues until the critical business functions re-established, and company's operation and business activities are restored. The major activities in this phase include: **notification and assembly of the recovery teams, implementation of interim procedures, and re-establishment of company's operation and business activities.**

3. Restoration

This phase consists of any and all activities necessary to make the transition back to a normal business operation.

D. Communication during disruption

During major disruptions, Information will be shared by Crisis Management Team, with periodic updates, where relevant. Communications with general public will be done by CISO. In case of strikes/ bandhs, Head of Admin will be requested to arrange for protection of assets and stationed personnel if the need is felt.

In case of planned disruptions, or for prolonged periods of downtime due to maintenance activities, email communication to be sent to all users, by the respective Head of Departments.

Section III: Recovery Teams

A. Purpose and Objective

This section of the plan identifies who will participate in the recovery process for the company's operation and business activities Business Continuity Plan. The participants are organized into one or more teams. Each team has a designated team leader and an alternate for that person. Other team members are assigned either to specific responsibilities or as team members to carry out tasks as needed.

Recovery Team Descriptions

This section lists the team definitions for the Recovery Teams and gives a short explanation of the function of each team or function.

References: **Appendix C – Recovery Team Descriptions & Assignments**

C. Recovery Team Assignments

This section identifies the team roles and the specific responsibilities that have been assigned to the team.

References: **Appendix C – Recovery Team Descriptions & Assignments**

D. Personnel Notification

This section specifies how the team members are to be notified if the plan is to be put into effect by identifying who calls whom, and in what order.

Reference: **Appendix G – Critical Employee Contact List**

Appendix D – Notification Plan

E. Team Contacts

This section specifies how the team members are to be notified if the plan is to be put into effect by identifying who calls whom, and in what order.

Reference: **Appendix G – Critical Employee Contact List**

Appendix F – Vendor List

Section IV: Recovery Procedures

A. Purpose and Objective

This section of the plan describes the specific activities and tasks that are to be carried out in the recovery process for company's operation and business activities. Given the Business Continuity Plan outlined in Section II, this section transforms those strategies into a very specific set of action activities and tasks according to recovery phase.

The recovery phases are described in **Section II. C** of the Plan.

Each activity is assigned to one of the recovery teams. Each activity has a designated team member who has the primary assignment to complete the activity. Most activities also have an alternate team member assigned.

B. Business Continuity

This section specifies how the recovery activities are to be carried out.

Reference: **Appendix E – Business Continuity Overview**

Section V: Appendices

Appendix A – Categorization of Disaster Events & Impact Appendix

B – Recovery priorities for Business Functions Appendix C –

Recovery Team Descriptions & Assignments Appendix D –

Notification Plan Appendix E – Business Continuity Overview

Appendix F – Vendor List Appendix G – Critical Employee Contact List

Appendix A: Categorization of Disaster Events & Impact

#	Probabilistic Event or Incident	Process(es)	Impact classification and Effect on Departments
1	Fire - Loss/ damage to office building due to fire	Business Departments	Crisis, Human Life
2	Earthquake - Loss/ damage to office building due to earthquake	Business Departments	Crisis, Human Life
3	Bandhs / lockdowns - Inaccessibility to Data centre/Office due to Bandh, employee strike, flood, pandemic, etc.	Business Departments	Major
4	Power Failure	Business Departments	Major
5	AC Failure	Business Departments	Major
6	Data Centre Network Unavailable for, ERP, other applications	Business Departments	Major
7	Hacking Attack / Virus Attack	Business Departments	Major
8	System Failure: ERP	Business Departments	Major, Finances
9	System Failure: Email	Electronic Communication across Company	Minor
10	System Failure: Data Centre CCTV & Access Control	Data centre	Minor

Negligible: No significant cost or damage

Minor: A non-negligible event with no material or financial impact on the business

Major: Impacts one or more departments and may impact outside clients

Crisis: Has a major material or financial impact on the business

Minor, Major, & Crisis events should be documented and tracked to repair

Appendix B: Recovery Objectives

#	Business Process	Critical Resource	Recovery Objective
1	Power failure	Generator Set	12 Hrs
2	Network Not available	Computer System	2 Hrs
3	System Failure - e-mail	Responsible for oversight of the hacking attack / virus attack recovery functions.	8 Hrs
4	ERP Recovery Team	Responsible for oversight of the ERP and recovery function	4 Hrs
5	System Failure – Virus	Responsible for oversight of the hacking attack / virus attack recovery functions.	12 Hrs
6	Pandemic	Critical contact teams are responsible for disaster management and recovery plan including VPN, Server and ISP management	24 Hrs

Appendix C: Recovery Team Descriptions & Assignments

#	Recovery Team	Description	Assignment
1	Crisis Management Team	This team is responsible for providing information regarding the disaster and recovery efforts to: Cellcomm's Senior Management Customers Vendors/Contracts Media Regulatory Agencies Other Stakeholders	Mr. Shibu Paul Mr. Kalyan Kumar PV Mr. George Mathews Mr. Santhosh PR Mr. Abhiraj P
2	Admin Management Team	Responsible for oversight of the power, Genset, AC, CCTV & Access Control recovery functions.	Mr. Kalyan Kumar PV Mr. Ganesh NA
3	IT Management Team	Responsible for oversight of the Data Centre Network availability for ERP, and other network applications.	Mr. George Mathews Mr. Prakash MR Mr. Tojimon Joseph
4	Man Made Disaster Recovery Team	Responsible for oversight of the hacking attack / virus attack recovery functions.	Mr. George Mathews Mr. Kumar A
5	ERP Recovery Team	Responsible for oversight of the ERP and recovery function	Mr. Prakash MR Mr. Tojimon Joseph Mr. George Mathews

Appendix D: Notification Plan

#	Probabilistic Event or Incident	Who will inform	Whom to inform
1	Fire - Loss/ damage to office building due to fire	Crisis Management Team	Fire Services
2	Earthquake - Loss/ damage to office building due to earthquake	Crisis Management Team	Fire Services
3	Bandhs / Lockdown - Inaccessibility to Data Centre/Office due to Bandh, employee strike, flood, pandemic etc.	Crisis Management Team	Security Services / Police / Hospital
4	Power Failure	Crisis Management Team	BESCOM
5	Data Centre Cooling Failure	Crisis Management Team	AMC Vendor
6	Data Centre Network Unavailable for, ERP, other applications	Crisis Management Team	IT Dept
7	Hacking Attack / Virus Attack	Crisis Management Team	IT Dept / Cyber Crime
8	System Failure: ERP	Crisis Management Team	IT Dept / ERP Team
9	System Failure: Email	Crisis Management Team	IT Dept
10	System Failure: Data Centre CCTV & Access Control	Data Centre	Admin Team / AMC Vendor

Appendix E: Business Continuity Overview

Criticality Class	Probabilistic Event or Incident	Procedure for Handling
Critical	System Failure – Server	All data can be recovered from tape through restoration process.
Vital	Failure of Network	Invoke SLA provisions with AMC vendor
Vital	Electronic mode of communication within the organisation – Email	Invoke SLA provisions with AMC vendor
Vital	Electronic mode of communication within the organisation - Electronic Sabotage	<ul style="list-style-type: none"> Antivirus software updation as a preventive measure^[SEP] Restoration of relevant data from backup if required
Vital	Gen Set Failure	Perimeter Access Restriction Awareness / Signages

Critical: Cannot be performed manually. Tolerance to interruption is very low

Vital: Can be performed manually for very short time

Sensitive: Can be performed manually for a period of time, but may cost more in staff

Non-sensitive: Can be performed manually for an extended period of time with little additional cost and minimal recovery effort

Appendix F: Vendor List

#	Goods / Service Provided	Vendor Name & Address	Contact Name & Phone	Vendor side Support Contact
1	Govt.Class-1 Licensed Electrical Contractors	M/s GTTC Electricals	Madhukeshav D.R- 9449719739	9449719739
2	Software Reseller & IT services	LDS Infotech Pvt Ltd	Mr. Krishna Kishore K- 9845354949	9845354949
3	SERVER	DELL INDIA PVT LTD	Mr. Rangesh- 91-44- 27158101	91-44-27158101
4	Fire alarm, Access control	OCIMUM SYSTEMS PVT LTD	Jayakumar	88612 99993
5	DG	Maniranjan diesel sales & service pvt ltd	SADAHIVA- 9513617568	9513617568
6	Web Hosting	hostgator.in	0824-6614102	0824-6614102
7	Leased line	Airtel	1800102001	1800102001
8	Leased line	Vodafone	1800-123-123-123	1800-123-123-123
9	Firewall	Sophos	000 800 100 8381	000 800 100 8381
10	AC	Blue Air Solutions Pvt Ltd	Mr.Imran Pasha- 9663344666	8884443717

Appendix G: Critical Employee Contact List

#	Service / Name	Contact Number	Responsibility Area
1	Thyagarajababu G T	9986070686	CSL- Health & Safety
2	Kalyan Kumar P V	9916907991	CSL – Admin & CISO
3	Sudha	9538809691	CSL – HR
4	George M	8884453427	CSL – IT
5	Prakash MR	9739973543	CSL – R & D
6	Shibu	9886792437	CSL – Technical
7	Abhiraj	9986019742	CSL – Production
8	Santhosh PR	9916919355	CSL – Sales
9	Suraj	9873355303	CSL – Technical