Ddev Plastiks Industries Limited

CIN: L24290WB2020PLC241791
Registered Office: 2B, Pretoria Street, Kolkata- 700 071

BUSINESS CONTINUITY POLICY

1. PURPOSE & SCOPE

Organizations face many risks from threats such as natural disasters like – fire, flood, terrorism, operational breakdowns, hostile political situations, virus attack etc. These threats can result in loss of profits, injuries, life, and damage to an organization's reputation, or in extreme cases, the end of the organization. Business Continuity Plan (BCP) ensures continuity of critical business processes after disaster and facilitates rapid recovery measures to reduce the overall impact of a potentially devastating business interruption.

The BCP includes the disaster management plan and the purpose of the plan is to allow for continuity of business operations at all facilities of Ddev Plastiks Industries Limited ("Ddev" or "the Company") in the event of an emergency, to facilitate business, resilient to potential disruptions and to recover affected business activity, if any, at minimal time. The plan provides adequate information on preventing and limiting the consequence of untoward incidents and handling emergency situations, if any. These procedures are aimed primarily at serving as guidance for the Emergency Response Team ("ERT") at plant/ unit level who are responsible for managing the employees/ workers to safety during time of crisis.

2. SHORT TITLE & APPLICABILITY

The company is committed to maintaining continuity of its business activities with an objective of continued value delivery to its stakeholders. This shall be achieved through continuance of business activities in face of disruptions (natural/man-made) with minimal impact on business performance/services, safety and security.

The Policy extends to the entire company, its subsidiaries, units, factories, offices and to all employees and workers. All Local Area Network, Servers, Equipment, Power, People-safety in the office premises/ units are covered by BCP, identifying the potential consequences of undesirable events and the safeguards needed to counteract their effects. Safeguards included in the BCP must be selected based on whether they are needed to maintain a minimum level of operation for the affected systems.

The BCP does not address specific disaster events. It is written for generic situation(s), which assumes that the site is suddenly inaccessible or must be vacated without warning. The nature of any incident and the severity of the restrictions it places on the company's operation cannot be known in advance. However, the relevant parts of this BCP should be used whether the incident either:

a) Closes the facility
b) Closes part of the facility
c) Prevents a major emergency

The BCP activities shall in no way jeopardize the other active Policies of the company.

3. OBJECTIVE

The objectives of BCP are:

a) To mitigate the possible impact of an interruption to the activities
b) To allow for continuity of operations by minimizing the effects of emergencies on people, property and environment in the company
c) Protect company's assets and employees from damage caused due to emergency situation
d) Implement procedures to minimize economic losses from disruptions to business operations
e) Identify critical operations and resume them at earliest possible in case of an emergency
f) Prepare an action plan for recovery of operations and identify key individuals to facilitate implementation of the plan
g) Provide safe working condition
h) Reduce risk by introducing better management practices.

4. ASSUMPTIONS

The following assumptions are made in the BCP:

- Key personnel and/ or their backups identified are available
- Recovery location(s) and facilities, as required, are available that can handle the specified recovery activities
- Vital resources including backup media and other immediate requirements, identified in the strategy, required for BCP, are available at the respective recovery location
- BCP shall not apply to non-recoverable situations such as global disaster
- BCP should not be invoked for addressing day to day failures like link or system failure.

5. BUSINESS CONTINUITY POLICY METHODOLOGY

The methodology for developing Business Continuity Policy (BCP) consists of eight separate phases, as described below. The company would take all the measures mentioned in this document to provide a minimum level of BCP in the company.

A. Phase-I: Pre-Planning Activities

This phase is used to obtain an understanding of the existing and projected computing environment of the company. Two other key deliverables of this phase are –

- The development of a policy to support the recovery programs; and
- An awareness program to educate management and individuals.

B. Phase-II: Identification of Assets and Vulnerability/Risk Assessment

Security and Control within the company is preferable, from an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing the impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence and includes the following key tasks –

- A thorough Security Assessment of the computing and communications environment including:
    1. Personnel practices
    2. Availability of skilled personnel
    3. Physical security
    4. Operating procedures
    5. Backup and contingency planning and procedures
    6. Access control software security
    7. Security planning and administration
    8. Personal computers
- Documentation of the findings and recommendations resulting from the findings of security assessment so that corrective action may be initiated in timely manner.
- Purchasing recovery planning and maintenance softwares, if any required, to support the development of plans and to maintain them following implementation.
- Developing plan frameworks
- Assembling team members and conducting awareness programmes

C. Phase-III: Business Impact Analysis (BIA)

This phase enables

- Accessing the economic impact of incidents and disasters that result in denial of access to systems services and other services and facilities.
- Accessing the length of time business units can survive without access to systems, services, and procedures; and
- Identification of the risks applicable for the systems, services and facilities and quantification of risks.

The risks deduced shall be guiding factor for the managerial decisions and corresponding risk mitigation measures. This shall help identify critical service functions and timelines in which they shall be recovered after interruption and according to the criticality of the service, maximum response time shall be identified along with the associated repair and recovery time.

D. Phase-IV: Detailed Definition of Requirements

During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analyzing alternative recovery strategies. Identifying resources required to support critical functions identified in Phase-III is used in developing this profile. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

E. Phase-V: Plan Development

During this phase, recovery plans components are defined, and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery Teams, their roles and responsibilities. Recovery standards are also developed during this phase.

F. **Phase-VI: Testing/ Exercising Program**

The plan Testing/Exercising Program is developed during this phase. Testing/ Exercising goals are established, and alternative testing strategies are evaluated. Testing strategies tailored to the environment are selected and on-going testing programs are established.

G. **Phase-VII: Maintenance Program**

Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect new changes to the environment. It is critical that existing change management processes are revised to take updated recovery plan maintenance into account. In areas where change management does not exist, change management procedures shall be recommended and implemented.

H. **Phase-VIII: Initial Plan Testing and Implementation**

Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following:

- Defining the test purpose/approach
- Structuring the test
- Conducting the test
- Analyzing test results
- Modifying the plans as appropriate.

6. BUSINESS CONTINUITY IMPLEMENTATION PROCESS

A. Risk Assessment and Business Impact Analysis

Risks can be broadly categorized into:

- Willful damage
- Poor System Performance including hardware and/or software failures, data corruption, link failure, network failure, malware, virus or other software attacks/ threats, hacking, non-availability of spares
- Heavy Rain/ Volcano/ Earthquake/ Floods/ Global warming, sea level increase, ozone depletion, heat waves, hurricane, tornado, biodiversity loss, soil erosion, Other Environmental/ Climate risks and/or natural disaster
- Strike/ Bandh/ Lockdown
- Water Scarcity/ Water Stress Risk
- Leakage of confidential information
- Electrical disturbance (surge, spike, short circuit, power failure, explosion, transformer spill, etc.)
- Fire
- Pests, Rodents
- Attrition
- Theft
- Unauthorized access

- Existing system flaws
- Release of hazardous material
- Arson and sabotage

B. Identification of Critical Services/ Functions

Critical functions are those functions that must be performed by the company to survive. Failure to perform them would result in serious or irreparable harm to the company. Impact may take the form of increased operating costs, loss of revenue collection, or inability to provide services to clients. The identified critical services are prone to the above-mentioned risks. The Business Impact Analysis needs to be carried out for each of the critical services. The cost impact shall be analyzed during the business continuity planning process preferably following the company's budgeting and business planning process for each department/ unit.

C. Categorization of Disaster

The identified critical services can be subjected to the following categories of disasters:

- Catastrophic Disaster: A catastrophic disaster is one in which the outage will probably last more than seven days. Damage due to a catastrophic disaster is severe and could involve total destruction of the company's facilities. Replacement of equipment or significant renovation of the facility may be necessary.
- Major Disaster: A major disaster is one in which the outage will probably last from two to seven days. Damage due to a major disaster is more severe than that due to a minor disaster but less than catastrophic disaster.
- Minor Disaster: A minor disaster is one in which the outage will probably last longer than one shift, but less than two days. Damage due to a minor disaster is comparatively light.

D. Classification of Assets

Company's assets may be classified as follows:

- Human Resources
- Information (Soft copies/ printed or hardcopies copies)
- Software (including applications, systems and third-party software), Hardware and Networks
- Fixed Assets
- Movable Assets
- Stocks/ Inventories

E. Loss of Assets

In the event of loss of asset(s) the person concerned will communicate the incident and the details of the lost asset to the ERT Leader through an Email or Letter, who in turn shall take necessary action.

F. Contingency Plan

The Contingency plan to continue the business activity, regardless of its size or scope of operation, should, as a minimum, address the following three elements:

- Emergency Response– Emergency response procedures to cover the appropriate emergency response to a fire, flood, civil disorder, natural disaster, bomb threat, virus, or any other incident or activity, to protect lives, limit damage, and minimize the impact on business operations.

- Backup Operations– Backup operations procedures to ensure that essential data processing/ operational tasks can be conducted after disruption to the primary data processing facility.
- Recovery Actions– Recovery actions procedures to facilitate the rapid restoration of a data processing facility/ operations following physical destruction, major damage, or loss of data.

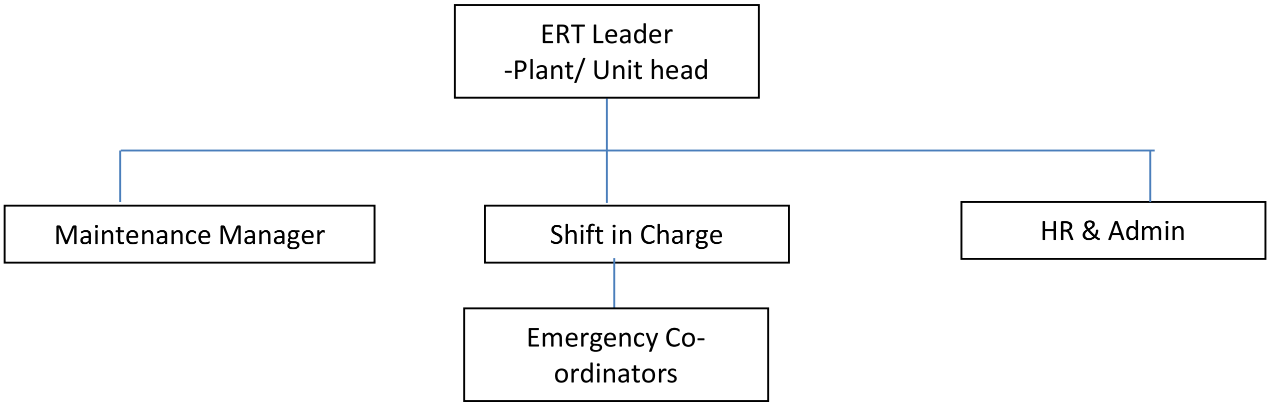
G. Escalation, Recovery and Business Resumption Process

A disaster recovery/business resumption plan is a comprehensive statement of actions to be taken in response to a disaster. It includes documented, tested procedures that, if followed, will assure the availability of the critical resources and facilities required to maintain continuity of operations. The strategy shall include identifying alternative safe storage areas, storing copies of original in various locations, off-site storage, backup materials/ data/ information, alternate processing capabilities, displaying emergency contact details, restoration mechanism of critical supplies and mechanism and state the steps to be followed for escalating unresolved to disaster status. The Emergency Response Team (ERT) shall be identified and problem escalation procedure be defined, including identifying command centers (ERT Leader) and executives to do the recovery and restoration.

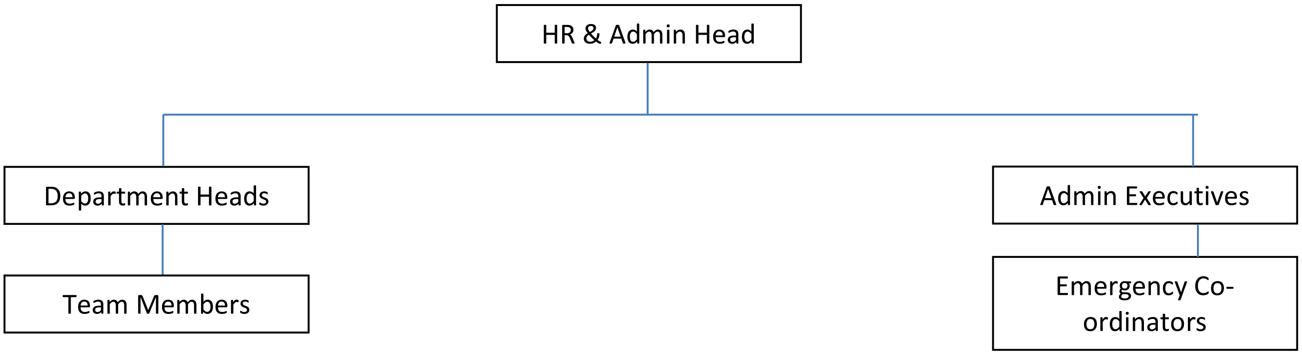
7. EMERGENCY RESPONSE TEAM

The company has identified an emergency response team (ERT) to enable effective management of emergency situations.

A. At Plant/ Unit Level



B. At Office



C. For Information Technology (IT) matters

The IT Department shall be immediately notified incase of possible or actual disaster or threats who shall in turn contact the department/ process/ unit head to assess the vulnerability and impact and plan data retrieval, safety, restoration and resumption strategy based on applicable policy.

8. INITIAL RESPONSE TO AN INCIDENT

The initial response may be as follows, however deviation thereto may be considered based on the severity and requirement:

- In case of danger to personnel, ensure the safety of employees/ workers/ staff/visitors/ any other people or life.
- Protection and safeguarding of business function and assets of the company
- Contact the emergency services / emergency response team
- Determine the extent of disruption
- Assess the expected time lapse/ re-occurrence chances prior to restoring the ability of the company to do business (completely or partially)
- Activate IT Disaster Recovery Procedure, Switch off electrical systems, arrange water, remove flammable or explosive materials, arrange firefighting systems, as deemed necessary
- Determine best means of communication
- Contact the unit/department head
- Restore, arrange, or make available necessary resources, computer systems, networks, communications, assets, data, professionals at alternate site as a part of quick and effective business resumption.
- Contact the CFO to alert insurers, factory inspector etc.
- Contact the HR & Admin Head to alert investigators, local administrators etc.
- Report the incident to authorities, if required.
- Launch an investigation into the cause of the incident

9. EMERGENCY RESPONSIBILITIES

Enlisted below are the general guidelines and responsibilities of the Emergency Team:

A. At Plant/ Unit

Emergency Team	Responsibility
ERT Leader-Plant/ Unit Head	To mobilize external/ internal resources and to instruct

	maintenance manager, HR & Admin and Shift-In-Charge and co-ordinate with them.
Maintenance Manager	To plan and make mobilization with HSE and electrician/ IT/ Control room in charge/ fire station/ firefighting team/ security/ factory incharge/ controller of stocks or explosives, others to restrict impact and ensure safe disposal/ removal of explosives or potential hazards.
HR & Admin	To make arrangements for the emergency response and evacuation along with coordinating with external agencies and making available the internal resources and ensure welfare and security, law and order and manage hospital coordination, ambulance, medical/ first aid facilities, transportation etc.
Shift-In-Charge	To initiate the Initial Response to the Incident and bring the incidence to the notice of ERT Leader and assist the maintenance manager To coordinate with local authorities/ facilitation centers/ hospitals and arrange for emergency/evacuation services/ facilities
Emergency Coordinators	To support in carrying out the responsibilities such as firefighting, rescue, rehabilitation, transport, and provide essential support and services.

B. At Office

Emergency Team	Responsibility
HR & Admin	To mobilize external/ internal resources and to instruct the department heads and admin executives and coordinate with them.
Admin Executives	To plan and make mobilization with electrical department/ electrician/ IT/ Office or building in charge/ fire station/ firefighting team/ security/ others to restrict impact and ensure safe disposal/ removal of explosives or potential hazards and ensure welfare and security, law and order and manage hospital coordination, ambulance, medical/ first aid facilities, transportation etc.
Department heads	To co-ordinate with team members and bring the incidence to the notice of HR & Admin and instruct the team members for safe and effective handling.
Team members	To initiate the Initial Response to the Incident and bring the incidence to the notice of ERT Leader and assist the Department Heads, Admin Executives and HR & Admin.

NOTE: During normal working hours the Plant/ Unit head will lead the Emergency situation however before/ after the normal working hours the shift-in charge and security officer will act as an Incident controller.

C. For Information Technology (IT) Issues:

Emergency Team	Responsibility
IT Team Head	To mobilize external/ internal resources and to instruct the

	department executives and admin executives for data/information retrieval, collection, alternate storage, resumption of processes.
IT Team Executives	To follow the procedure and instructions for data/information retrieval, collection, alternate storage, resumption of processes.

10. EMERGENCY COMMUNICATION

Immediately after the emergency event, the Emergency Team shall be notified and shall implement business recovery operations as per the business continuity policy and disaster management plan.

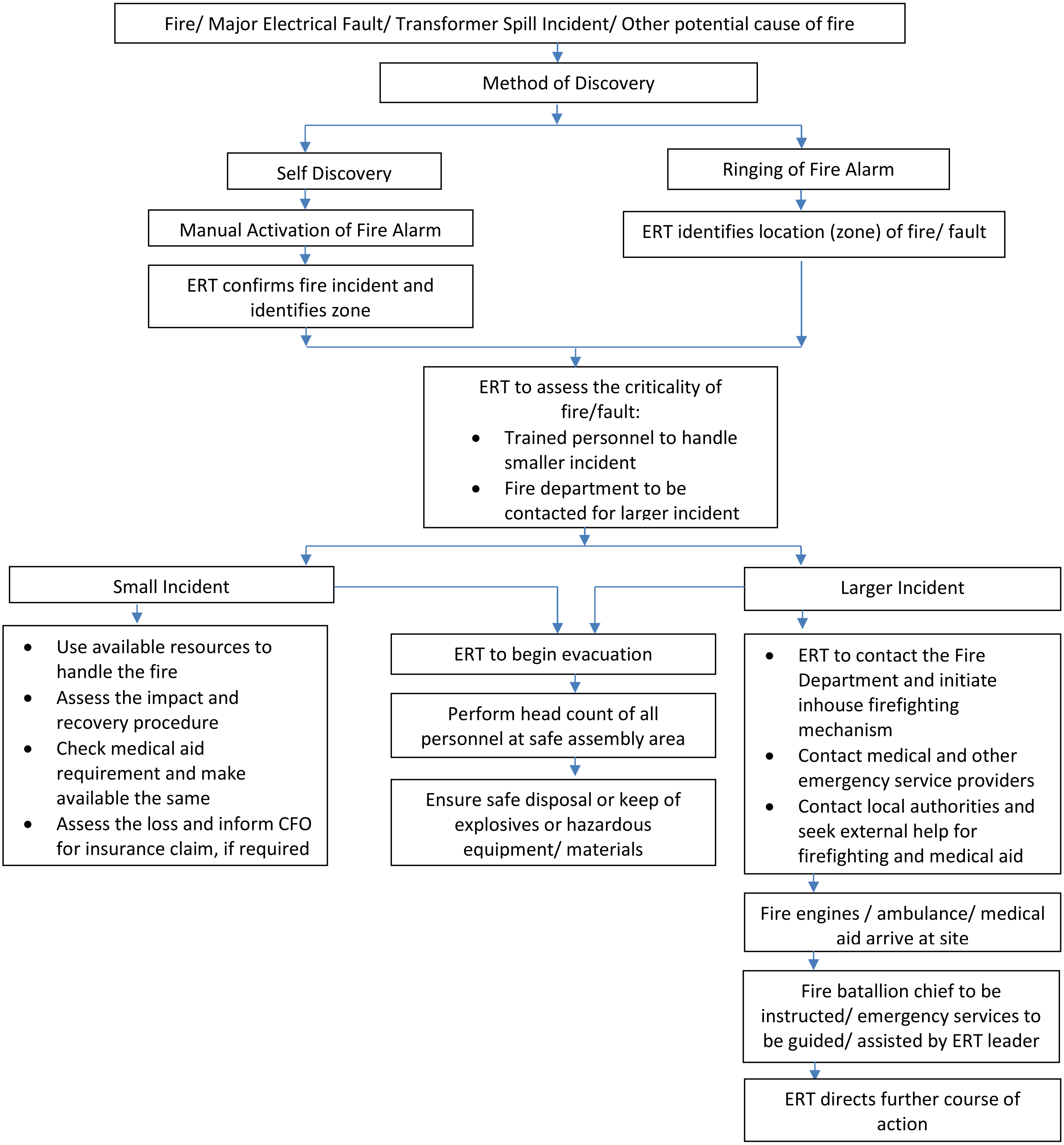
11. EMERGENCY PREPAREDNESS PLAN

All units/plants/offices/ facilities are equipped with the following

- Fire suppression system-all plants/ units/ offices/ facilities are equipped with the fire suppression system as well as fire detection system as per the statutory norms.
- Fire hydrant systems
- Fire jockey pump/ main electrical pump/ fire diesel engine
- Draw out valve/ Hose reel/ fire extinguishers/ sand buckets/ water monitor
- First aid boxes
- Fire alarm systems
- Fire sprinkler system
- Personnel protective equipment/ gears
- Manual alarms/ hooters
- Face Masks, Protective Gears

12. EMERGENCY ACTION PLAN

A. For handling fire incident/ Major Electrical Faults/ Arson and Sabotage:



Fire/ Major Electrical Fault/ Transformer Spill Incident/ Other potential cause of fire

Method of Discovery

Self Discovery

Manual Activation of Fire Alarm

ERT confirms fire incident and identifies zone

Ringing of Fire Alarm

ERT identifies location (zone) of fire/ fault

ERT to assess the criticality of fire/fault:

- Trained personnel to handle smaller incident
- Fire department to be contacted for larger incident

Small Incident

- Use available resources to handle the fire
- Assess the impact and recovery procedure
- Check medical aid requirement and make available the same
- Assess the loss and inform CFO for insurance claim, if required

ERT to begin evacuation

Perform head count of all personnel at safe assembly area

Ensure safe disposal or keep of explosives or hazardous equipment/ materials

Larger Incident

- ERT to contact the Fire Department and initiate inhouse firefighting mechanism
- Contact medical and other emergency service providers
- Contact local authorities and seek external help for firefighting and medical aid

Fire engines / ambulance/ medical aid arrive at site

Fire batallion chief to be instructed/ emergency services to be guided/ assisted by ERT leader

ERT directs further course of action

B. For Earthquake

a) ERT personnel to use hooter alarm in case of earthquake

b) ERT personnel to ensure employees drop to the floor and take shelter under a heavy piece of furniture against an inside wall away from the glass windows until shaking stops

c) Evacuate immediately when shaking stops to prevent injury/ damage due to after-shocks.

C. For Floods/ Cyclones/ Heavy Rain/ Sea Level Increase/ Hurricane/ Tornado:

a) ERT Personnel to monitor the situation/ weather forecasts and recommend appropriate preventive measures

b) Take preventive actions as per IMD advisory

c) Move all portable equipment to certain height

d) Operators to be trained to properly cover equipment with protective plastic covers as required.

D. For Disaster Management in other climate/ environmental/ civil/ human risks:

a) Provide medical assistance to injured. (**Do not move seriously injured persons unless they are in immediate danger of further injury)**

b) Inform the necessary emergency services like fire brigade and medical services

c) Shut off all power and check for obvious structural damage

d) Check for any resulting hazards such as fires, exposed/arcing electrical components/wires, leaking sewage, broken water pipes, dangling fixtures/ furnishings

e) Begin search and rescue operation, if required

f) Be prepared for aftershocks, which can cause additional damage

g) ERT shall ensure people do not leave for home or re-enter the facility without being instructed to do so

h) Incase of visible serious damage, arrangements to be made with a professional structural engineer to inspect offices and buildings following the disaster in order to determine whether or not its safe to re-enter or continue to operate within.

E. For Willful Damage/ Theft/ Strike/ Bandh/ Lockdown/ Water Scarcity/ Pest and/or Rodents Issue/ Unauthorized Access/ Attrition/ Minor Electrical Fault/ Hazardous Material Leak:

a) The Department/ Unit head or shift in charge or person aware of such incidents may report to senior management/ ERT Leader and HR and Admin Head

b) The exit and entry of person/ loss of material (in case of theft/ willful damage/ unauthorized access/ attrition) shall be restricted by the ERT Team/ available executives.

c) The ERT Leader shall ensure peaceful assembly/ status quo in case of Strike/ Bandh/ Lockdown.

d) The HR Head/ Admin shall ensure water availability in case of water scarcity and arrange for pest control and disinfectants in case of pest and/or rodent attacks.

e) The electrical department/ electrician shall be informed by the Shift In charge or HR & Admin in case of minor electrical fault.

f) Necessary protective gears should be made available to the persons involved amd adequate evacuation procedure should be initiated by the ERT in case of leakage of hazardous materials

F. For IT/ System Performance Issues/ System and/or network Failure/ Data Breach/ Data Loss Matters/ Malware/ Software Attacks:

#	Disaster Scenario	Responsibility	Impact	Recovery Procedure
1	**Server Down** Primary Domain Controller with DNS, DHCP and Active Directory Secondary Domain Controller with DNS, DHCP and Active Directory-Kolkata	IT Department	High	• Component level errors could be resolved by replacing the parts from AMC vendor or local stock. • In case of a complete crash - ○ One standby server is ready with complete configuration. ○ Connect the server in the network and resume the service.
	• Additional Domain Controller – Alternate Locations	IT Department	Low	• Inform vendor and get the device repaired
2	**Backup Device Down** • FTP Server • External Hard disk drive • Cloud Backup	IT Department	High	• Inform AMC vendor and get the device repaired • Take data from cloud Backup • If FTP server is down then we can get data from External Hard disk. Else the data we can get from FTP. • After repair, test the device and re-commission the same.
3	**Network Devices** Fortinet (Primary Network Appliance – All locations) All network devices have alternate backup devices	IT Department	High	• Inform Warranty vendor • Use standby module to support the affected segment • Replace/repair the faulty module
4	**Communication Links Down** • 10 Mbps ILL (1:1) Kolkata	IT Department	High	• Inform service provider • Use dial-up link as alternative

	- Internet Dongles as backup activity - Alternate ILL from other ISP as Backup - Internet Dongles as backup activity - Proposed another ILL of 02Mbps from other ISP as Backup.			- Restore the link and resume normal service
5	**Power Supply Devices Down**			- Inform AMC vendor - Keep only critical machines ON - Transfer load to other UPS
7	**Physical Security Devices Down** - CCTV System	Admin Department	Medium	- Inform AMC vendor - Deploy guards at all strategic positions

13. EMPLOYEE AWARENESS AND TRAINING:

The company shall, from time to time, conduct detailed training schedules for all employees regarding the BCP, ensuring awareness of their roles in various disaster scenarios. Evaluate training outcomes through periodic drills and quizzes to measure understanding.

14. REVIEW AND UPDATION

The BCP shall be reviewed at such intervals, as deemed necessary by the Risk Management Committee and Board of the Company which may recommend any amendments/ modifications/ revisions and/or discontinuation of any or all the provisions of the policy. The revision shall be in line with the changing regulatory framework and business dynamics, as well as the expectations of stakeholders. The Chairman and Managing Director is empowered and authorized to interpret and clarify the provisions of the policy in case of any doubt/ ambiguity. In case of any contradictions with statutory guidelines in this regard the said may prevail over the policy.