MDI NetworX Private Limited

Business Continuity Plan

Version 2.2

Document Release Note

This Business Continuity Plan (BCP) is for MDI NetworX Private Limited henceforth called as MDI NetworX or organization, with 8717 West 110th St, Ste 480 Overland Park, KS 66210, US and 717 East Ordnance Road, STE 208 Baltimore, MD 21226 and delivery center at 601, Delta-2, Giga Space, Viman Nagar, Pune – 411014, India Revisions, if any, to this plan will be sent to each person holding a copy. Comments, suggestions or queries will be addressed to the BCP Manager.

Document Identification	
Document Owner:	*Dhanashri Oza*
BCM Manager:	*Dhanashri Oza*
Approved By:	*Alpana Sharma*
Document Name:	MDI NetworX Business Continuity Plan
Supporting Document Directory Path:	MDI NetworX BCP Annexures
Draft approved on:	*16th Mar'21*
Document Classification:	Confidential

Document Version Control				
Version	Release Date	Author	Reviewer	Change(s)
1.0	16-Mar-21	Amar Uttarkar	Alpana Sharma	Original Document
1.0	01-Apr-22	Amar Uttarkar	Alpana Sharma	Annual Review; No changes proposed.
2.0	03-Jan-23	Amar Uttarkar	Alpana Sharma	Change in Document Distribution List
2.0	28-Oct-23	Dhanashri Oza	Alpana Sharma	Annual Review; No changes proposed.
2.1	15-Oct-24	Dhanashri Oza	Alpana Sharma	Annual Review; Replaced Simran with Prashant as a BCM Coordinator.
2.2	12-May-25	Dhanashri Oza	Alpana Sharma	Annual Review; Replaced Himanshu with Aman, Sujata with Khushboo, and Pramod with Ninad as a BCM Coordinator.

Document Distribution List		
Name	Designation/ Department	Role
Alpana Sharma	CTO	BCM Steering Committee Head
Partha Bose	COO	Alternate Steering Committee Head
Dhanashri Oza	Associate Director – Compliance & Audit	BCM Manager
Aman Rajput	Software Development	BCM Coordinator
Khushboo Verma	Sr. Director - Quality Assurance	BCM Coordinator
Sushil Badola	AVP - Operations	BCM Coordinator
Abhijit Pardeshi	Director - Information Technology	BCM Coordinator
Ninad Kulkarni	Director	BCM Coordinator
Prashant Kulkarni	SVP - Talent & Administration	BCM Coordinator
Sridhar Iyer	Associate Director – Admin	BCM Coordinator

Content

1 Introduction

A Business Continuity Plan (BCP') signifies the preparedness of an organization to ensure continuity of critical business processes at an agreed level while limiting the impact of disaster incidents on people, processes and infrastructure.

Disasters and disruptions can occur without a warning and the results could be unpredictable. Events may occur, which can take weeks or months, even years for an organization to recover from the outage caused by disasters. It is important to build a level of resilience in the business operations in order to minimize the effects of such disruptions. A robust and well maintained BCP ensures the recovery of business operations when confronted with adverse events such as natural and man-made disasters.

The purpose of this document is to enumerate the mission critical activities performed at MDI NetworX, Pune, India and Baltimore, MD and Overland Park, KS, US analyze possible disaster threats and resulting outage scenarios, and devise strategy to resume business operations in an outage scenario.

The plan highlights the procedures to be followed in the event of disaster scenarios caused by disaster incidents and the resources which are necessary to resume business operations during such times. These predefined procedures are not to be interpreted as the only course of action. In some cases, they will be superseded by common sense or modified to suit the particular disaster incident and outage scenario.

2 MDI NetworX – Location overview

2.1 Location covered under the scope

Primary Center:
8717 West 110th St, Ste 480 Overland Park, KS 66210

Secondary Center:
717 East Ordnance Road, STE 208 Baltimore, MD 21226

Backup Center:
AWS, US East coast (N.Virginia)

2.2 Physical Security

Floor reception and guards also man the entrance to the working area to ensure that only authorized persons are permitted inside the office area. Access card readers are installed at all the critical entry and exit points of the office premises to ensure that physical access is provided only to authorize personnel. CCTV cameras are installed at all the entry and exit points. Also, CCTV cameras are installed in the office premises. CCTV cameras are also installed where critical IT equipment is located. The premises security is recorded 24x7.

2.3 Fire Safety

Fire extinguishers are installed in the working areas of MDI NetworX. Fire extinguishers are maintained by third party vendor which are monitored by MDI NetworX branch administration on a regular basis. Security guards at each floor are trained to use fire extinguishers.

2.4 Emergency Exits

In the event of a disaster, employees are always advised to use the emergency exit doors. MDI NetworX has emergency exits at each floor in branches of all locations. Multiple emergency exit signage and evacuation plan are present at the floor to guide the staff towards the emergency exits in the event of a disaster.

2.5 Safe or Assembly Areas

Safe or Assembly areas are designated areas that have been established for employees in case of a disaster incident. These areas are designed to move employees away from areas of potential danger at the site, and to establish a location to determine if all employees have been safely evacuated from the affected areas. Safe assembly point is located opposite to the entrance to A1 building on 1st Floor in India office and Parking zone in US office.

2.6 Information Technology Infrastructure

The IT team of MDI NetworX performs the below IT infrastructure activities for MDI NetworX:

- Tech support
- Server Management
- Network Management
- IT Security
- Logistics and procurement
- Business application support ERP
- Business application support Legacy Systems
- Web Applications Support

- Third Party Application Support
- Database Management

Primary data center is located at *Overland Park, KS* and IT DR is located at AWS, US East coast (N.Virginia), where data and application replication are performed.

The key components and processes that form the building blocks of the IT Security Architecture at MDI NetworX are as under:

- Endpoint Security on all user computers
- Operating System Hardening
- Comprehensive IT Policies
- Unified Threat Management based Firewall
- Content & Universal Resource Locator (URL) based filtering
- Anti-Spam System for email
- Intrusion Detection Systems – IDS (internal and external facing)
- Intrusion Protection Systems – IPS
- Advanced Persistent Threat (APT) System
- Centralised Security Operations Centre
- System Patch Management System
- Security Information and Event Management (SIEM) System
- Demilitarised Zone for all Internet facing services
- Rule based vulnerable application blocking at firewall layer

Backup of Database and other required folders/files

IT team performs daily incremental backup and full backup once in a week so that the information can be protected and can be accessed easily. The backups are stored at US office location. The backups are encrypted so that no one else can access the files/data. Below is the list of important files for which the backup shall be taken once in a week:

- Database
- Important folders of Finance team
- Important folders of HR
- SVN
- Important folders of operations and MIS

3 Scope

Scope Inclusion

The scope of this BCP document is limited to the recovery of MDI NetworX business processes functional from MDI NetworX located at Pune, India, and Baltimore, MD and Overland Park, KS, US and the critical IT applications that are supporting these critical business processes.

The document covers following core business departments:

- Software Development
- Quality Assurance
- Operations
- Mailroom and scanning (US)

The Document covers following critical Support Departments

- Information Technology
- Admin (Corporate Services & Facilities)
- Legal
- Human Resource

The Document covers following critical Support functions

- Legal
- Finance
- Media Management

The document includes detailed sections on Business Impact Analysis (BIA'), Recovery Time Objective (RTO'), Disaster Threat Analysis and Employee Safety Measures, Recovery Strategy and Procedures, Emergency Response Teams (ERTs'), Function Recovery Teams (FRTs'), BCP Training, BCP Testing; and BCP Governance and Maintenance.

Scope Exclusion

The BCP document shall not address continuity issues arising out of limited outages (e.g. fire in a small section of premises, etc.) or planned outages (e.g. those resulting from periodic maintenance of UPS systems or offline backup of systems etc.)

Risk- Acceptable level

MDI NetworX has defined the acceptable level of risk for the continuity of services provided to stakeholders. The decision of acceptable level of risks for the business has been taken by its Senior Management based on business' risk appetite. The key acceptable risks are:

- **MDI NetworX Processes:** BCMS Plan do not address processes categorized as Moderate critical or below in business impact analysis process. Recovery for these categories of processes would be on best effort basis by the process owners.
- **Third party vendor processes:** Plans assume that the third-party vendors will recover the critical processes within Recovery Time Objective (RTO) as agreed with the respective business owner of MDI NetworX.

4 Objectives

The primary purpose of this plan is to ensure safety of people, respond to any crisis and minimize the impact to business.

The high-level intent of this document is:

- To provide safety to people (Full time, temporary staff working in MDI NetworX premises).
- To support MDI NetworX employees, assets and business in the event of disruption and ensure that critical activities continue in an event of the disaster.
- To minimize financial and operational losses due to non-availability of critical business processes and IT systems during a crisis situation. To ensure that critical business operations and IT systems continue in the event of a crisis.
- To minimize the inconvenience and potential disruption to customers and stakeholders.
- To minimize the impact to MDI NetworX's public and industry image during a crisis.
- Comply with the statutory and regulatory requirements, to the extent possible.

5 Key Assumptions

The following assumptions have been made while formulating the BCP:

- Overall losses, in many cases are likely to be far greater in the event of actual disaster. It should be noted that due to the inherent limitations of a risk assessment exercise, it is never possible to quantify the full impact of such a scenario. Therefore, intangible losses have been considered while assessing the impact.
- It has been assumed that staff and skills will be available for recovery. Without relevant people, premises, general infrastructure, IT infrastructure and support recovery is not possible.
- The plan is based on various disaster scenarios envisaged. However, it does not include special situations that may occur. Some examples include country wide incident/war, simultaneous break down of all vital citywide infrastructure, etc.
- Vendors will provide the requisite services; and if required, the Service Level Agreements (SLAs) with vendors are modified to include clauses related to service levels for managing continuity risks.
- SLA will be formalized with third parties/vendors to ensure required support (including infrastructure, networking, security, application and other facilities) at disaster recovery location(s).
- If, during an event, these conditions cannot be met, implementing a workaround or substitute will be a top priority to facilitate further activation of the plan.

a. Facility:

I. Access to the backup facility or any other alternate facility would be made available in 1 working day by Admin.

II. Computers/Laptops along with internet access would be made available in 1 working day at the temporary location by IT.

III. Any vital records/documents for operations processes can be made available within 1 working day by the IT.

b. People:

I. Transportation of associates or other resources to be managed by admin.

II. At least one representative from BCP Committee to be made available.

III. The scope of the event is such that lack of prompt and effective action may result in impacts on MDI that are intolerable, causing lasting and significant damage to the company.

c. Business:

I. All links, applications to be made available in 1 working day by the IT team.

II. Access to all network folders to be made available in 1 working day by IT team.

III. All-important folders are backed-up on weekly basis by IT team.

IV. Critical equipment like laptops, internet, and dongles would be made available in 1 working day by Admin / IT team.

d. Areas of Vulnerability

This plan has the following areas of vulnerability and single points of failure:

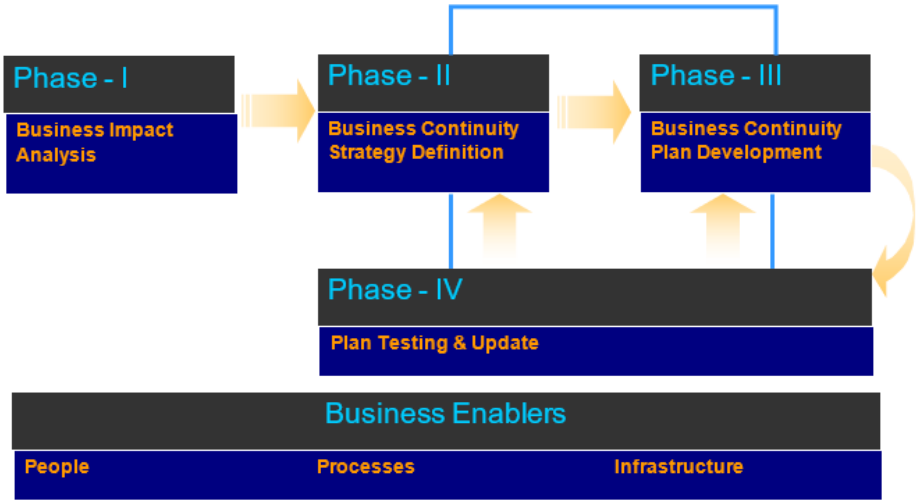
I. Small team size of the Operations team may limit the ability to reassign work and maintain response capabilities during long duration events, increasing the likelihood of responder fatigue, burnout and errors.

II. In case of any major disruption the Operations team will have to stretch and do all the work and activities they have been specified.

III. IT & admin recovery priorities and capabilities should be validated with training BCP.

6 Methodology

The following Methodology has been used to develop the BCP for MDI NetworX:



The specific tasks that were performed in each of the phases shown in methodology are listed below:

Phase I
Business Impact Analysis phase involved following tasks:

- Document agreed upon overall BCP expectations of MDI NetworX management.
- Develop a work plan with key milestones.
- Review documented business processes and identify critical business processes based on the impact analysis.
- Review existing disaster combat measures and backup procedures.

Phase II
Continuity Strategy phase involved following tasks:

- Develop continuity strategy for critical processes.
- Identify recovery site location.
- Identify minimum resources required for resumption of services at recovery location.

Phase III
Continuity Plan Development phase involved following tasks:

- Identification of ERTs and procedures to be followed by these teams in the event of a disaster resulting in an outage scenario.
- Assist in conducting initial awareness training for these teams.

Phase IV
Plan Testing and update phase involved following tasks:

- Develop a framework for the initial awareness tests among general associates and ERTs.
- Paper walkthrough of the plan.
- Establish governance and maintenance framework of the plan.

7 Business Impact Analysis (BIA) and Risk Assessment

The main objective of Business Impact Analysis (BIA) is to assess the possible impact to business processes due to disruptions as a result of an extended outage.

Recovery Time Objectives (RTO) is the period of time within which the business processes have to be resumed after an outage at an agreed level. The objective of setting RTO is to ensure that services to clients are not disrupted beyond agreed timeframes in the event of an outage scenario resulting from disaster incidents.

The various processes that have been identified for BIA are detailed in following:

7.1 Summary of BIA

Business Impact Analysis is the base document for evaluating different mitigation/recovery options and decide the appropriate strategy/strategies to be adopted, which will be used to prepare the Business Continuity Plan. Based on our discussions with the BCM coordinators of each department the business impact analysis was conducted to gather information and assign criticality, recovery point objectives, and recovery time objectives, resource requirements, dependencies, and vital records. Below is the summary.

Sr. No.	Department	Business RTO	Business RPO	IT RTO	IT RPO
1	Software Development	3 days to 1 Week	24 Hrs	24 hrs	24 Hrs
2	Quality Assurance	Up to 1 Day	24 Hrs	24 hrs	24 Hrs
3	Operations	Up to 3 days	24 Hrs	24 hrs	24 Hrs
4	Mailroom and Scanning	Up to 3 days	24 Hrs	24 hrs	24 Hrs
5	Information and Technology	>4 Hours ≤ 8 Hours	24 Hrs	24 hrs	24 Hrs

7.2 Criticality of business processes

All the business function processes of MDI NetworX are classified in this section on the basis of their criticality. The process criticality is determined on the basis of operational, financial, reputational, regulatory, contractual obligations, competitive advantage and stakeholder's confidence impact to MDI NetworX in case of disruptions to respective processes. The process criticality matrix shown below provides the results of process criticality analysis.

Criticality	Number of Processes
High Critical	2
Medium Critical	15
Low Critical	10
Total	**27**

Refer Annexures for List of Critical Processes for detailed business process criticality analysis.

Criticality	Description
High Critical	A process with RTO of **up to 1 day** is defined as critical. Disruption of this process will have significant impact on the organization.
Medium Critical	A process with RTO of **more than 1 day and up to 3 days** is defined as moderate critical. Disruption of this process will have moderate impact on the organization.
Low Critical	A process with RTO of **more than 3 days, up to 1 week and more than 1 week** is defined as low critical. Disruption of this process will have low impact on the organization.

7.3 Summarized Recovery Time Objective

Recovery Time Objectives (RTO) is the period of time within which the business processes have to be resumed after an outage at an agreed level. The objective of setting RTO is to ensure that MDI NetworX services to clients are not disrupted beyond agreed timeframes in the event of an outage scenario resulting from disaster incidents.

Recovery Time Objective (RTO)	Number of Processes		
	High Critical	Medium Critical	Low Critical
Up to 30 minutes	--	--	--
> 30 Minutes ≤ 2 Hours	--	--	--
>2 Hours ≤ 4 Hours	--	--	--
>4 Hours ≤ 8 Hours	--	1	--
Up to 1 Day	1	--	--
Up to 3 Days	--	15	--
> 3days ≤ 1 week	--	--	2
More than 1 week	--	--	8

7.4 Threat Assessment and Employee Safety Measures

7.4.1 Introduction

A key section of the BCP process is the assessment of the potential risks of disruptions in business arising from disasters or emergency situations. It is necessary to consider all the possible incidents and the impact such situations may have on the organization's ability to continue delivering its normal business services. This section of the BCP will examine the possibility of serious situations disrupting the business operations and the potential impact of such events.

7.4.2 Threat Assessment

Disaster is an event that can negatively impact business operations of an organization for a short term or a prolonged duration. A disaster resulting in an outage scenario, often causes partial or complete stoppage of work and may impact only a particular function or all the functions operating from a specific facility of the organization.

In this section of the document, various types of disaster events are analyzed for potential threat to the organization and likelihood of their occurrence. Disasters like nuclear warfare are not addressed by this BCP document as probability of their occurrence is very low in this geographical reason based on historical information. Each potential disaster threat under the following headings is reviewed to arrive at the threats to be addressed in this document:

7.4.3 Environmental Disasters

- Fire
- Flood
- Food and water contamination
- Epidemic
- Drought
- Earthquake
- Tsunami
- Heat Wave

7.4.4 Organised and/or Deliberate Disruption

- Terrorist attack/ Hostage incident
- Bomb threat
- Transport strike
- Employee strike

- Riots / Bandh
- Physical security breach
- Logical security breach (Data)
- Physical damage to premises
- Risks associated with neighbours

7.4.5 Loss of Utilities and Services

- Power outage
- Failure of public & private transport system
- Water supply failure
- Denial of access to site
- Loss of key customers

7.4.6 Equipment or System Failure

- System outage
- Heating/Ventilation/Air Conditioning failure
- Breakdown in communications infrastructure

7.4.7 Others

- Third party liability
- Compliance failure

All the disaster events are rated on a qualitative basis considering:

- their overall impact on resources (people, physical infrastructure and technology) required for conducting normal business operations
- likelihood of their occurrence
- availability of response
- forewarning
- duration

8 Recovery Strategy Framework

MDI NetworX shall and implement appropriate recovery strategies to obtain and operate resources required for critical function recovery in accordance with the risk appetite. All recovery strategies should be formulated keeping in mind the six R – Reduce, Respond, Recover, Resume, Restore and Return that is, being able to:

- Reduce an impact of a BC event
- Respond to a BC event
- Recover from a BC event
- Resume critical business processes after a BC event
- Restore the primary site after a BC event
- Return to normal operations

8.1 Identification of Critical People, Facilities and Technology

Based on the input of Business Impact Analysis, critical people, facilities and technology are determined for critical processes. Key considerations for the Minimum Operating Requirement (MOR) shall include:

- People;
- Information and data;
- Buildings, work environment and associated utilities;
- Facilities, equipment and consumables;
- Information technology and telecommunications systems;
- Transportation;
- Finance; and
- Vendors.

8.2 Communication with Department Personnel

- All reporting managers shall have each of their reporting associate's contact information.
- Admin personnel shall list each member's contact information, including alternate or home methods if available.
- First responders and senior team members in each team will ensure that all personnel are evacuated or directed to the appropriate on-site shelter areas.
- Managers need to account for each of their employees using visual verification or other means of checking in.
- Managers need to communicate status with their employees on where they should go and what they should be doing.
- Managers need to report the status of their teams to their Incident Management Team representative.
- Since there are only 30 laptops assigned for BCP use, the reporting managers shall plan to work in 3 different shifts of eight hours each so that there is no loss in the production. Even if there is some loss due to the environment and the unforeseen system issues, is shall be minimal.
- In addition to the laptops assigned for the BCP, the supporting staff/managers shall provide their laptops if there is any requirement.

Notification Process/Call Tree

- Upon notice or notification of a potential business disruption, the department member will attempt to contact BC coordinator/ BC Manager by sending an email to CIMT@MDINetworX.com

Notification Process:

- The concerned person will first contact Alpana Sharma (+919960582681) by calling her on her official mobile number as mentioned below

- In case she is not reachable on her cell, the member should leave a SMS for the contact attempt and include the reference to the next persons Dhanashri (+917391094900) and Prashant (+919112200880) who will be contacted.
- In case Dhanashri / Prashant is not reachable, the member should leave a SMS for the contact attempt and include the reference to the next person Abhijit (+919011036942) and Prasad (+919552588517) who will be contacted.

8.3 Resource/Alternate Facility Analysis and Recovery Strategy

Formulation

The identification of dependency of the process on the people is the key input to the formulation of recovery strategy. The dependency can be removed by one of following:

- Documentation of the action steps in which critical processes are performed;
- Training of critical processes within the team
- Cross training of critical processes to the people in other processes
- More than one person should have the knowledge of core skills e.g. provisioning, making entry to the technical systems, creating invoices, reports, etc.
- Knowledge retention and management, so that identified fallback member can continue the process in the unavailability of primary critical resource.

The risks to the IT applications, network components and links are identified and mitigated. The dependency on the application, network components and links as a single point of failure is removed by selecting appropriate workaround to continue the operations till the application, network component and link is recovered.

8.4 Recovery Strategy Selection

The following parameters are considered while selecting the recovery strategies:

- Feasibility: Feasibility of adopting the recovery strategy.
- Establishing Time: Expected time to establish the recovery strategy.
- Cost of establishment of recovery strategy: Expected cost of establishing the recovery strategy v/s impact if the process is down.
- Dependency on vendors / legal / regulatory bodies.

8.5 Recommended Recovery Strategies

Following is a list of recovery strategies which can be used as a full-blown recovery strategy or a work-around to be combined with other strategies to recover the work of the primary site.

- Option A – Displacement Strategy (Workload Distribution (WLD)/ Split Operation)
- Option B – Remote Access (Work from Home (WFH))
- Option C – Alternate Location (People Relocation to Alternate Locations)
- Option D – Training (Cross Training between two Teams)
- Option E – Disaster Recovery (DR) Site (IT DR site)

The implementation one or more of the above-mentioned recovery options by MDI NetworX will be purely based on the client's business requirements.

8.5.1 Option A - Displacement Strategy (Workload Distribution (WLD)/ Split Operation)

Description

Displacement Strategy (Workload Distribution/Split Operation) is a recovery strategy where in the operations are distributed across two or more operating locations working on the same process. This recovery strategy will work along with one or more strategy options (like cross training, work from home etc.). This recovery strategy leverages on Organization's multi-location presence. No additional costs are incurred.

Suitability

- Recovery time objective is very short (e.g. Up to 8 hrs).
- Covers Contingency till 72 hrs.
- Inter-City or Intra City relocation of personnel is not possible (e.g. city-wide flooding /earthquakes).
- No or less logistical cost as compared to other strategies.

8.5.2 Option B – Remote Access (Work from Home (WFH))

Description

Remote Access (Work from home) is a recovery strategy where in certain key personnel or BCP identified personnel will be provided with laptops and peripherals, loaded with all the required applications so that they can work from home in case of contingency.

Suitability

- Processes present at only location of organization.
- People cannot reach office, and RTO is short (e.g. 4 hrs).
- Less number of people required to recover the process.
- Quick communications with the Customers.

8.5.3 Option C – Alternate Location (People Relocation to Alternate Locations)

Description

Utilizing other branch offices / Alternate locations as a DR Site is a recovery strategy wherein alternate space can be utilized, and recovery of the processes is achieved. Agreement with the alternate to provide seats to resume the mission critical operations will be required.

Suitability

- Processes present at only location of organization.
- Recovery more than 72 hrs.
- Recovery not possible at the location.
- Low-capacity mission critical processes.

8.5.4 Option D - Training (Cross Training between two Teams)

Description

Cross training between other teams is more of a work-around along with other recovery strategies. In Cross training FTEs of two different sub-processes or two different functions are trained on the processes which are critical. This helps the critical processes of the down functions to be managed by contingency functions / recovery team.

Suitability

- If Workload Distribution (WLD) is used as recovery strategy and process has major deviations.
- Other less-critical process staffs are going to recover the process located in other branches.

8.5.5 Option E – Disaster Recovery (DR) Site (IT DR site)

Description

Presence of DR site for IT recovery in geographically segregated location to recover from failure at primary site. This could be implemented by physical Data centres at two different locations may be different vendors. In case the organization switches to cloud services, request will be placed with the cloud service provider for recovery.

Suitability

- Customer facing applications, where availability requirements are 24X7.
- Data protection requirements due to nature of business and regulatory requirements.

Recovery strategy should be formulated by considering failure scenarios associated to the identified critical enablers:

Scenario	Facility	People	Technology	Probable Reasons	Possible Recover Strategy
Business As Usual	✓	✓	✓		Preventive Strategies / Risk Management
Site/facility unavailable	×	✓	✓	• Electricity/ HVAC Failure • Fire in premises	• "Hot Site" – A disaster recovery site • Workload Distribution • Work from Alternate location • Work from home • Transfer of operations to off city
Critical people at primary site unavailable	✓	×	✓	• Social unrest (riot/ bandh, terrorist attack). • Epidemic/ Pandemic • Natural disaster (floods, earthquakes)	Workload Distribution • Cross Trained FTE pool between two teams (work as a team against in silo) • "BCP FTEs" - Pre-approved BCP FTE pool • Transfer of operations to off city • Urgent hiring • Temporary staff
Applications / IT / Network components unavailability	✓	✓	×	• Failure of ISP links • Cyber-attacks (DDoS, Ransomware) • Loss of data centres • Critical applications/ equipment failure	Workload Distribution • Cross trained FTE pool between two teams (work as a team against in silo) • Work from home • Invoke DR • Virtual private Network • Manual workarounds
Multiple or All resources at primary Site unavailable	×	×	×	• Social unrest (riot/bandh, terrorist attack). • Natural disaster (floods, earthquakes)	Workload Distribution • Cross trained FTE pool between two • teams (work as a team against in silo) • "Hot Site" – A disaster recovery site

Recovery Strategies	Recovery Options	Pros	Cons
Remote Access	Work from home	• Continued Operations • Employees can work remotely in case of the epidemics • No maintenance of workspaces for staff	Provide below facilities: • VPN • Laptops • Data cards • Mobiles • Emails • Printing facility (New Business) • Transportation for staff • Vital records (Letter heads, Rubber stamp etc.)
Alternate Location	Use of alternate office locations	• Synergy will be achieved by regrouping staff under one roof, thus enabling better management of operation. Easier flow of information among the staff in times of crisis. This leads to better decision making and efficiency • Highest Resilience and rapid recovery of operations	• Setting up and maintenance of an alternate site with all necessary resources to facilitate recovery activities will necessitate considerable investments
Displacement Strategy	Split operations	• Workload distributed during normal BAU • Continued seamless operations during disaster	• Investment costs - setting up the alternate office with all the necessary resources and continuous maintenance of the facility • Regular adequate training and working understanding of the business processes to ensure continuity of operations in times of disasters • Increased Manpower / Productivity
Disaster Recovery (DR) Site	IT disaster recovery site	• Availability of critical IT systems (high availability)	• Maintenance of an IT DR site with all necessary IT Infrastructure to facilitate IT recovery will necessitate considerable investments
Training	Cross training	• No additional cost • Continued operations during disaster	• Continuous trainings and more frequent exercises • Managing during employee attrition • Efficiency

8.6 Outage Scenarios

Many disaster incidents have common consequences resulting in a loss or temporary exclusion from a key resource, e.g. site exclusion can be caused by fire or explosion, or flood that causes a total or partial destructive loss of buildings and facilities. The outage scenarios considered for recovery are therefore any business interruption events resulting in a prolonged outage of, or exclusion from key business resources. In a worst-case scenario, the occurrence of the disasters mentioned above may lead to the following outage scenarios:

8.6.1 Premises are not accessible

This outage scenario would result from a disaster incident like Bomb Threat, Earthquake Tremor, Flood, Small Fire or Riots. This scenario presents a situation where due to disaster incidents mentioned above, the premises have been declared inaccessible by building management / regulatory authorities. This outage of this nature could result in a short to medium term outage (less than 5 days), or a long-term outage if the premises are declared unfit to use due to structural damage after initial survey.

8.6.2 Premises are destroyed

This outage scenario would result from a major disaster incident like Fire (accidental / arson) or Earthquake and may have severe impact on human resources besides affecting physical and technology infrastructure. The premises could be partially / completely destroyed and may be declared inaccessible / unavailable for a prolonged duration because of structural damage, personnel safety or regulatory reasons i.e. police inquiry, insurance survey etc.

8.6.3 IT systems are unavailable, but premises are accessible

This outage scenario would result from disaster incidents like Power Outage or System Outage. This outage scenario does not pose a threat to premises and human resources, however due to heavy dependence on technology, business operations may come to a grinding halt.

8.6.4 Human resources are not available

Human resources are most critical component of any operation. Disaster incidents such as Food & Water Contamination and Flood could result in loss/injury to life, while situations such as transport / employee strike may lead employees not been able to reach the workplace. This is a severely damaging scenario, since recruitment and training of human resources is a time-consuming process.

8.7 Recovery procedures

The following recovery actions are to be used as a guide. During a real disaster circumstances may dictate that some or all of the steps documented may have to be altered. The HoD/ department BCM coordinator should use his/her judgment while managing the recovery operation.

1. The HoD/ department BCM coordinators shall call the BCM Steering Committee Head to give the details of the impact of the disaster on his/her department.

2. The HoD/ department BCM coordinator shall call a meeting of key department personnel to determine actions to be taken and establish the priority of restoring critical functions based on the readiness of alternate location and resources available.

- Review tasks to be performed and assign personnel.
- Personnel should be assigned to contact vendors and advise them about the situation and when they can expect service to be restored. Use the Vendor Notification in the appendix for contact information.
- Determine if some personnel will have to travel to the alternate/recovery site.
- Distribute copies of any forms that will be needed during the recovery operation.

- Personnel should be assigned to provide recovery support needed by other teams, as needed.
- Identify the category in which personnel should be alerted. Consider:
  I. Personnel that might be needed to give aid to other teams / departments.
  II. Personnel that will be needed at the alternate location to resume normal business functions.
  III. Personnel who should stay home and remain on standby.

3. Contact personnel that will be needed to report to the assigned alternate location.

4. Designate space for personnel reporting to the alternate location.

5. Implement procedures to resume time dependent functions based on the priority established.

6. As progress continues during the recovery operation, the team should be prepared to move back to the affected facility and resume normal business operations.

Acronym	Details
BSC	BCM Steering Committee
ERT	Emergency Response Team
AST	Administration Support Team
EST	Employee Support Team (HR Team)
FRT	Function Recovery Team
FST	Finance Support Team
ITRT	Information Technology Recovery Team
LRMT	Legal Risk Management Team
MMT	Media Management Team
SRT	Salvage Recovery Team

8.7.1 Premises not accessible

The activities that are to be performed in an outage scenario 'Premises not accessible' have been listed below. Detailed action steps falling under each key activity mentioned herein for every team are documented in the Business Continuity Teams section of the BCP document. Activities with the two asterisk (**) signs against them need to be performed simultaneously after the BCP has been invoked.

Continuity actions (Premises not Accessible)	Responsibility
Disaster endured for 0-1 days. If the disaster occurs impacting the accessibility of premises for 0-1 days following steps will be performed	
Evacuation and first-aid	
1. Raise the alarm	ERT
2. Facilitate evacuation procedures	ERT
3. Liaise with Emergency Response Authorities and seek assistance to combat the disaster.	ERT
4. Facilitate assembly of employees	ERT
5. Provide first – aid measures	ERT
6. Assembly roll call	ERT
7. Inform BSC	ERT
Assessment and disaster announcement	
1. Initial Assessment	ERT/ AST

Continuity actions (Premises not Accessible)	Responsibility
2. Disaster announcement	BSC
3. Reporting to key stakeholders	BSC
Initiate Relocation	
1. Plan the resumption process	BSC
2. Relocation to the contingency location	AST
3. Open communication channels	BSC
4. Initiate onsite support from client (where applicable)	FRT
5. Gather information	FRT
6. Activate relocation procedures	FRT
7. Disseminate information	ERT
8. Activate IT infrastructure at contingency location	ITRT
9. Contact third party service providers (where applicable)	ITRT / FRT
10. IT systems and data recovery	ITRT
11. Procuring additional IT infrastructure (if required)	ITRT
12. Activation of basic facilities at contingency location	AST
13. Coordinate resumption activities at contingency location	AST
14. Urgent recruitment (if required)	EST
15. Facilitate emergency recruitment and training (if required)	EST
Assistance to employees (**)	
1. Assistance to employees / employees' families	EST
2. Organize counselling (if required)	EST
3. Compensation pay-outs (if applicable)	EST
Salvage Operations	
1. Assess the extent of the damage to the premises and equipment	SRT
2. Control physical access to damaged premises	SRT
3. Obtain information about insurance cover (if insured)	SRT
4. Preserve evidence	SRT
5. Initiate insurance claim (if applicable)	SRT
6. Regular reporting to BSC	SRT
Deployment of funds (**)	
1. Estimate fund requirements	FST
2. Arrange for funds	FST
3. Advances in lieu of salary (if required)	FST
Media management (**)	
1. Assemble the team	MMT
2. Draft communication	LRMT
3. Review draft communication	MMT
4. Liaise with the media	MMT
5. Instructions to employees	MMT
6. Formulate public relations plans	MMT
7. Activate communication channels	MMT
8. Website update	MMT
9. Monitor media	MMT
Public relations and long-term plan assessment (**)	

Continuity actions (Premises not Accessible)	Responsibility
1. Manage public relation activities	BSC
2. Evaluate existing and proposed business plans in the light of disaster	BSC
3. Report to key stakeholders	BSC
Legal formalities (**)	
1. Identify likely areas of litigation	LRMT
2. Liaise with legal advisor	LRMT
3. Liaise with regulatory authorities	LRMT
Recording events / expenses (**)	
1. Maintain records	BSC
2. Obtain information on fixed expenses	FST
3. Record recovery expenses	FST
Monitoring operations & Coordination (**)	
1. Liaise with ERTs	FST
2. Clean up affected location	AST
3. Collate information	AST
4. Monitor systems	ITRT

8.7.2 Premises destroyed

The activities that are to be performed in an outage scenario 'Premises destroyed' have been listed below. Detailed action steps falling under each key activity mentioned herein for every team are documented in the Business Continuity Teams section of the BCP document. Activities with the two asterisk (**) signs against them need to be performed simultaneously after the BCP has been invoked.

Continuity actions (Premises not Accessible)	Responsibility
Evacuation and first-aid	
1. Raise the alarm	ERT
2. Facilitate evacuation procedures	ERT
3. Liaise with Emergency Response Authorities and seek assistance to combat the disaster.	ERT
4. Facilitate assembly of employees	ERT
5. Provide first – aid measures	ERT
6. Assembly roll call	ERT
7. Inform BSC	ERT
Assessment and disaster announcement	
1. Initial assessment	ERT/AST
2. Disaster announcement	BSC
3. Reporting to key stakeholders	BSC
Initiate Relocation	
1. Plan the resumption process	BSC
2. Relocation to the contingency location	AST
3. Open communication channels	BSC
4. Initiate onsite support from client (where applicable)	FRT
5. Gather information	FRT
6. Activate relocation procedures	FRT

Continuity actions (Premises not Accessible)	Responsibility
7. Disseminate information	ERT
8. Activate IT infrastructure at contingency location	ITRT
9. Contact third party service providers (where applicable)	ITRT / FRT
10. IT systems and data recovery	ITRT
11. Procuring additional IT infrastructure (if required)	ITRT
12. Activation of basic facilities at contingency location	AST
13. Coordinate resumption activities at contingency location	AST
14. Urgent recruitment (if required)	EST
15. Facilitate emergency recruitment and training (if required)	EST
Assistance to employees (**)	
1. Assistance to employees / employees' families	EST
2. Organize counselling (if required)	EST
3. Compensation pay-outs (if applicable)	EST
Salvage Operations	
1. Assess the extent of the damage to the premises and equipment	SRT
2. Control physical access to damaged premises	SRT
3. Obtain information about insurance cover (if insured)	SRT
4. Preserve evidence	SRT
5. Initiate insurance claim (if applicable)	SRT
6. Assess the extent of the damage to the premises and equipment	SRT
Deployment of funds (**)	
1. Estimate fund requirements	FST
2. Arrange for funds	FST
3. Advances in lieu of salary (if required)	FST
Media management (**)	
1. Assemble the team	MMT
2. Draft communication	LRMT
3. Review draft communication	MMT
4. Liaise with the media	MMT
5. Instructions to employees	MMT
6. Formulate public relations plans	MMT
7. Activate communication channels	MMT
8. Website update	MMT
9. Monitor media	MMT
Public relations and long-term plan assessment (**)	
1. Manage public relation activities	BSC
2. Evaluate existing and proposed business plans in the light of disaster	BSC
3. Report to key stakeholders	BSC
Legal formalities (**)	
1. Identify likely areas of litigation	LRMT
2. Liaise with legal advisor	LRMT
3. Liaise with regulatory authorities	LRMT
Recording events / expenses (**)	
1. Maintain records	BSC

Continuity actions (Premises not Accessible)	Responsibility
2. Obtain information on fixed expenses	FST
3. Record recovery expenses	FST
Monitoring operations & Coordination (**)	
1. Liaise with ERTs	FST
2. Clean up affected location	AST
3. Collate information	AST
4. Monitor systems	ITRT

8.7.3 IT systems unavailable, but premises accessible

The activities that are to be performed in an outage scenario 'IT systems unavailable, but premises accessible' Premises not accessible' have been listed below. Detailed action steps falling under each key activity mentioned herein for every team are documented in the Business Continuity Teams section of the BCP document. Activities with the two asterisk (**) signs against them need to be performed simultaneously after the BCP has been invoked.

Continuity actions (I.T. systems unavailable, but premises accessible)	Responsibility
The Recovery Time Objectives for key Clients / Internal Functions supporting the critical processes have been agreed upon. The management will evaluate the reasons of IT systems unavailability and determine the duration for which the IT systems would remain unavailable. The recovery actions have been documented as follows:	
Disseminate Information	
1. Inform the BSC	FRT
Assessment and disaster announcement	
1. Initial assessment	ERT/AST
2. Disaster announcement	BSC
3. Reporting to key stakeholders	BSC
Initiate Recovery	
1. Plan the resumption process	BSC
2. Open communication channels	BSC
3. Initiate onsite support from client (where applicable)	FRT
4. Activate IT infrastructure at contingency location	ITRT
5. Contact third party service providers	ITRT
6. IT systems and data recovery	ITRT
7. Procure additional IT infrastructure (if required)	ITRT
Salvage Operations	
1. Obtain information about insurance cover	SRT
2. Insurance claim (if applicable)	SRT
3. Regular reporting to BSC	SRT
Deployment of funds (**)	
1. Estimate fund requirements	FST
2. Arrange funds	FST

Continuity actions (I.T. systems unavailable, but premises accessible)	Responsibility
Media management (**)	
1. Assemble the team	MMT
2. Draft communication	LRMT
3. Review draft communication	MMT
4. Liaise with the media	MMT
5. Instructions to employees	MMT
6. Formulate public relations plans	MMT
7. Activate communication channels	MMT
8. Website update	MMT
9. Monitor media	MMT
Public relations and long-term plan assessment (**)	
1. Manage public relation activities	BSC
2. Report to key stakeholders	BSC
Legal formalities (**)	
1. Identify likely areas of litigation	LRMT
2. Liaise with legal advisor	LRMT
3. Liaise with regulatory authorities	LRMT
Recording events / expenses (**)	
1. Maintain records	BSC
2. Obtain information on fixed expenses	FST
3. Record recovery expenses	FST
Monitoring operations & Coordination (**)	
1. Liaise with ERT	FST
2. Collate information	AST
3. Monitor systems	ITRT

8.7.4 Human resources not available

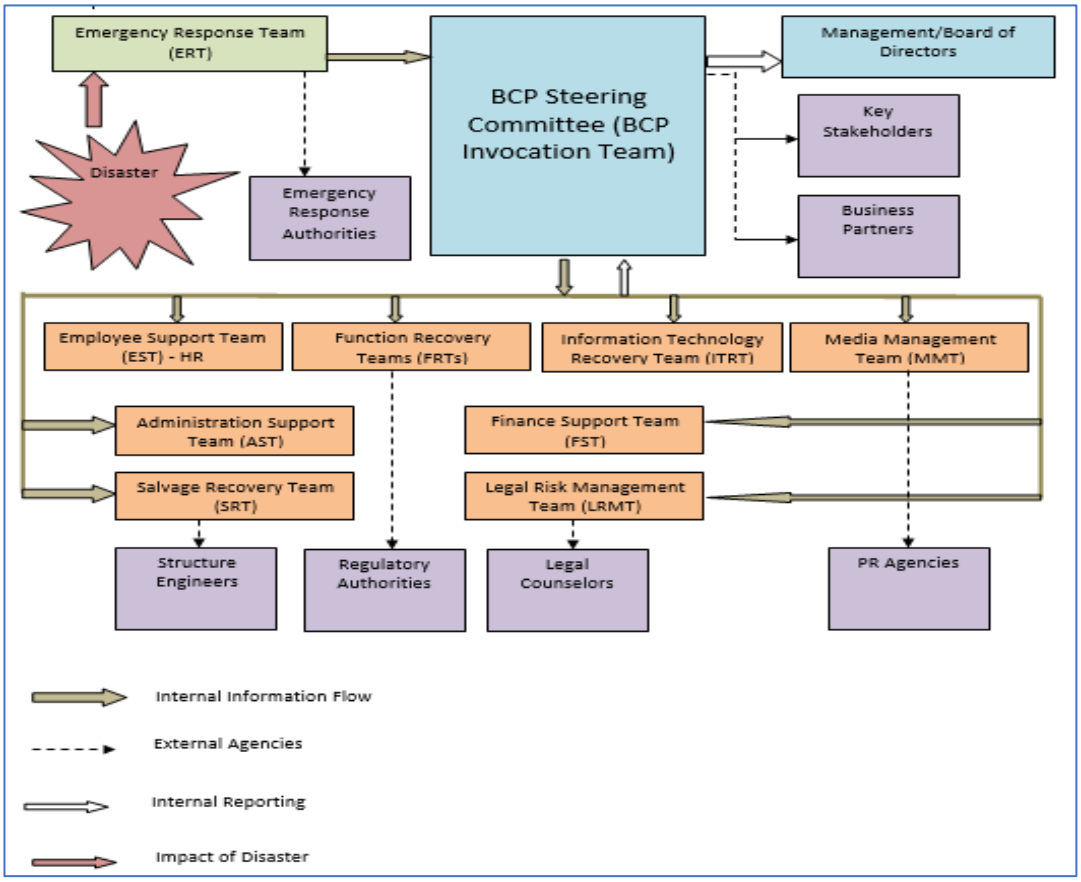
The activities that are to be performed in an outage scenario 'Human resources not available' have been listed below. Detailed action steps falling under each key activity mentioned herein for every team are documented in the Business Continuity Teams section of the BCP document. Activities with the two asterisk (**) signs against them need to be performed simultaneously after the BCP has been invoked.

Continuity actions (Human resources not available)	Responsibility
Evacuation and first aid	
1. Raise the alarm (in case of food and water contamination / flood)	ERT
2. Liaise with Emergency Response Authorities and seek assistance to combat the disaster	ERT
3. Provide first – aid measures	ERT
4. Inform BSC	ERT
Assessment and disaster announcement	
1. Initial assessment	ERT/AST
2. Disaster announcement	BSC

Continuity actions (Human resources not available)	**Responsibility**
3. Reporting to key stakeholders	BSC
Initiate Relocation	
1. Open communication channels	BSC
2. Initiate onsite support from client (where applicable)	FRT
3. Urgent recruitment (if required)	EST
4. Facilitate emergency recruitment and training (if required)	EST
Assistance to employees (**)	
1. Assistance to employees / employees' families	EST
2. Organize counselling (where required)	EST
3. Compensation pay-outs (If applicable)	EST
Salvage operations	
1. Assess the extent of the damage to the premises and equipment	SRT
2. Control physical access to damaged premises	SRT
3. Obtain information about insurance cover (if insured)	SRT
4. Preserve evidence	SRT
5. Initiate insurance claim (if applicable)	SRT
6. Assess the extent of the damage to the premises and equipment	SRT
Deployment of funds (**)	
1. Estimate fund requirements	FST
2. Arrange for funds	FST
3. Advances in lieu of salary (if required)	FST
Media management (**)	
1. Assemble the team	MMT
2. Draft communication	LRMT
3. Review draft communication	MMT
4. Liaise with the media	MMT
5. Instructions to employees	MMT
6. Formulate public relations plans	MMT
7. Activate communication channels	MMT
8. Website update	MMT
9. Monitor media	MMT
Public relations and long-term plan assessment (**)	
1. Manage public relation activities	BSC
2. Evaluate existing and proposed business plans in the light of disaster	BSC
3. Report to key stakeholders	BSC
Legal formalities (**)	
1. Identify likely areas of litigation	LRMT
2. Liaise with legal advisor	LRMT
3. Liaise with regulatory authorities	LRMT

9 Business Continuity Teams

In order to expedite recovery operations after occurrence of a disaster, the task has been allocated to a set of people who are identified and trained for the purpose. Business Continuity Teams are divided into small teams identified to perform pre-defined tasks. Each of the teams will perform specific tasks to facilitate timely resumption of business, limiting the impact on people, processes and infrastructure. The composition and size of these teams will vary with the size and geographical spread of the organization. The illustrative list of recovery teams is as depicted below:



The details of above-mentioned teams have been provided in the subsequent sections in the following structure:

• Team Name	Provides the title given to the Business Continuity Teams.
• Role	Provides an overview of the roles and responsibilities of the team.
• Pre-requisites, if any	Any requirements which the team should fulfil in order to perform its roles and responsibilities efficiently.
• Team Composition	Provides details of the members of the team as well as back-up members and their contact information.
• Key Tasks	Provides an overview of the key procedures that the Business Continuity Teams will perform during resumption.
– Action Steps	Provides information on actual work steps to be carried out by the team. These are recommended steps.
– Liaison	Provides cross reference to other internal and external teams with which the described team is required to liaise with. Also provides reference to annexure detailing information relevant for each team.

9.1 BCM Steering Committee (BSC)

Role

The BCM Steering Committee (BSC) shall assess initial impact of the disaster to decide if the BCP needs to be activated. The BCM Steering Committee (BSC) shall also be responsible for managing resumption activities. BSC will follow the principle of management by exception during the disaster and ensure that all Business Continuity Teams are empowered to execute the activities as per the BCP. The resumption and restoration activities may involve various critical decisions impacting resources and existing business plans. Therefore, the BSC will comprise of heads of departments and senior management personnel.

Pre-requisites for invocation of the BCP

The BCP will be invoked in the event there are reasons to believe that:

- the affected location and / or critical resources would be unavailable for the foreseeable future (typically more than one month)
- the operating efficiency of processes will be significantly impacted if business operations are required to be carried out from the affected location
- there is a high possibility that either of the above-mentioned situations arise

Team Composition

Based on current level of operations and number of associates, organization will maintain personnel in the respective teams.

Key Tasks

#	Key Tasks	Liaison
1	**Initial Assessment** Obtain information about the disaster and condition of the affected location from internal and authentic external sources to assess the extent of damage. Action Steps: • Acquire information from ERT and AST key personnel at the affected location. • Obtain evidence about devastation from authentic sources. • Conduct physical inspection of site, if possible and if permitted.	• ERT (Emergency Response Team) • AST (Administrative support team) • Key personnel at the affected location • Media/ Press • Emergency Response Authorities
2	**Disaster Announcement** Hold a meeting among BSC members to update them on the state of affairs and have a detailed deliberation before invocation of the BCP. Action Steps: • Convene a meeting of the top management to update them on the situation. • After obtaining necessary consent, if required, declare the disaster and activate the BCP. • Instruct the HODs to invoke contingency measures.	• HODs
3	**Regulatory Compliances** Complete formalities as may be warranted by any regulatory or internal policies.	• Regulatory Authorities • HODs

#	Key Tasks	Liaison
	Action Steps: • Pass an extraordinary board resolution in the same meeting to empower BSC to take charge of operations. • Complete formalities like obtaining written approvals / authorizations, if required, from parent organization and regulatory authorities.	
4	**Reporting to key stakeholders** Update key stakeholders on the disaster situation and the way forward for invocation of the BCP. Action Steps: • Communicate the incidents and activities currently underway to the key stakeholders.	• Group Company Directors • Key Stakeholders • Business Partners • Regulatory Authorities
5	**Assess the extent of disruption** Obtain information from HODs and ERT on the extent of disaster and estimated time for which the affected location will be unavailable. Accordingly guide the HODs to initiate operations for resumption. **Action Steps:** • Assess the extent of damage to the affected location. • Instruct the Business Continuity Teams to perform procedures at the affected locations as defined in the BCP.	• Board • ERT • All other Business Continuity Teams
6	**Relocation to the contingency location** Ensure that relocation to the contingency location has taken place as per the BCP and facilitate by solving bottlenecks, if any. **Action Steps:** • Ensure that AST and EST have identified resources for relocation to the contingency location. • Ensure that all other HODs have initiated response procedures.	• AST (Administration support Team) • EST (Employee Support Team) • All other Business Continuity Teams
7	**Open communication channels** Communicate on a regular basis with FRTs to obtain information on the recovery process and accordingly update key stakeholders on the same. **Action Steps:** • Obtain information from Emergency Response Authorities and relevant HODs on the extent of damage and status of all employees. • Design a reporting structure along with timing, whereby all recovery teams provide periodic updates to HODs. • Communicate with all stakeholders and top management on a regular basis to keep them updated on the recovery operations and latest developments.	• Emergency Response Authorities • FRTs (Functional Recovery Team) • Key stakeholders • Top management
8	**Maintain Records** • Document key activities carried out as a part of the recovery process and maintain relevant evidence.	

#	Key Tasks	Liaison
9	**Plan the resumption process** • Liaise with HODs and FRTs to plan the resumption process along with proposed time frames for each process. Consider the option of long-term relocation based on the condition of the affected location. **Action Steps:** • Prepare a recovery work plan along with target dates for resuming normal level of business operations. • Confirm with the HODs, LRMT and Structural Engineers whether the affected location can be used for conducting business operations. • If the affected location cannot be used for conducting business operations, organize relocation of business operations to alternate premises for a long-term basis.	• AST • Structural Engineers • LRMT (Legal Risk Management Team) • Business Continuity Teams • FRTs
11	**Arrange funds for resumption process** • Mobilize funds after assessing monetary requests made by different Business Continuity Teams for facilitating the recovery operations.	• Group Company Directors • FST
12	**Urgent recruitment** • Liaise with EST as well as FRTs to recruit personnel for vacancies created due to the disaster.	• EST • FRTs
13	**Manage public relation activities** • Contact key internal and external parties like key stakeholders, family members of affected employees and update them on the measures that MDI NetworX is taking to combat the disaster.	• MMT (Media Management Team) • EST
14	**Update the MDI NetworX authorities** • Update appropriate MDI NetworX authorities on status of recovery operations.	• Group Company Directors
15	**Evaluate existing and proposed business plans in the light of disaster** • Consider the impact of disaster on current or proposed business plans and accordingly revisit the timing of these plans.	• FRTs

9.2 Emergency Response Team (ERT)

Role

The Emergency Response Team (ERT) will be the first to face the disaster. The prime function of ERT shall support in safety of personnel through organized evacuation. The ERT comprises of mainly the administrative personnel and is led by a representative from the administration department.

Pre-requisites for the ERT

- The ERT members will be well acquainted with the premises structure and the surroundings.
- They will be trained in providing first-aid measures to affected personnel.
- The ERT members will also be aware of the procedures to be followed in order to liaise with various Emergency Response Authorities.
- The ERT will be aware of the “Do’s and Don’ts” during a disaster scenario.

Key Tasks

#	Key Tasks	Liaison
1	**Raise the alarm** • Raise the alarm as soon as the disaster occurs	
2	**Facilitate evacuation procedures** • In case the employees are in the office premises, initiate the building evacuation plan after considering the type of disaster.	• AST
3	**Liaise with Emergency Response Authorities** • Contact Emergency Response Authorities and seek assistance to combat the disaster.	• Emergency Response Authorities
4	**Facilitate assembly of employees** • Evacuate employees at the affected location and move towards the identified assembly area.	
5	**Provide first – aid measures** • Co-ordinate with all employees who have acquired specialized training in providing first-aid, Cardio Pulmonary Resuscitation (CPR), language skills, etc. for emergency situations to provide first aid or any other medical assistance to employees as maybe needed.	• EST
6	**Assist in providing medical attention to injured employees** • Facilitate speedy movement of injured personnel to hospitals, when the medical authorities arrive. • Organize for traumatized personnel to be counselled.	• EST • AST
7	**Assembly Roll Call** • Confirm whether all employees have successfully evacuated the affected location and reached the assembly location. **Action Steps:** • Perform a check for determining names of employees present during the disaster at the affected location. • Find out from employees who successfully evacuated the building regarding whereabouts of their colleagues at the time of disaster. • Conduct a roll call at the assembly location to confirm whether all employees have successfully evacuated the affected location. • Assist emergency authorities to identify bodies of employees who have died in the disaster.	• EST
8.	**Activate relocation procedures** Initiate relocation to the contingency location as per the BCP. **Action Steps:** • Communicate to the relevant contingency location about the disaster and tentative number of employees who need to be relocated to the	• FRTs • Personnel at the contingency location

#	Key Tasks	Liaison
	contingency location as per the BCP to enable them to make the necessary arrangements.	
9.	**Liaise with BSC** • Communicate to BSC to update them on details of the recovery operations.	• BSC

9.3 Salvage Recovery Team (SRT)

Role

The Salvage Recovery Team (SRT) will be responsible for assessing the damage caused by the disaster in order to estimate the monetary value of the loss due to the impact of the disaster and liaising with the insurance company to register the claims.

Key Tasks

#	Key Tasks	Liaison
1	**Assess the extent of the damage to the premises and equipment** • Visit the affected location after obtaining clearance from Emergency Response Authorities, to assess the premises and equipment for the extent of damage. • Ensure that the salvaged equipment is shifted to a safe area, outside the affected premises and their utility is evaluated • Liaise with the ITRT for the shifting of IT assets.	• ITRT (IT Recovery Team) • AST • Emergency Response Authorities
2	**Control physical access** • Make sure that entry to the affected location is limited to authorized employees and Emergency Response Authorities only. • Ensure that the physical security team deploys personnel at the affected location and security guards escort all visitors to the premises at all times	• AST • Security Service Agency
3	**Obtain information about MDI NetworX's insurance cover** Liaise with the administration department and FST to get information on the relevant insurance policies. **Action Steps:** • Obtain information about the following from the administration department: – Insurance Company – Type of Policy – Policy Number – Amount of coverage • Liaise with the accounts department and obtain original invoice copies for all assets for which insurance is being claimed.	• AST • FST (Finance Support Team)

#	Key Tasks	Liaison
4	**Preventive measures** • Obtain an opinion from safety workers and structural engineers and seal off areas which could be potentially dangerous for personnel safety.	• AST • Structural Engineers
5	**Preserve evidence** • Collect and maintain evidence which is found during the physical tour and may be useful to legal officials / Emergency Response Authorities. • If possible and permitted, take photographs / video shoot the location.	• AST
6	**Insurance Claim** • Contact the insurance agent / company to assess the damage to the physical location and assets. • File for insurance claim based on the assessment and insurance coverage.	• FST • AST
7	**Recovery operations** • Make sure that AST does not undertake recovery operations until clearance has been obtained from insurance company and Emergency Response Authorities.	• AST
8	**Regular reporting to BSC** • Update BSC on a regular basis about the ongoing salvage operations.	• BSC

9.4 Media Management Team (MMT)

Role

The Media Management Team (MMT) is responsible for ensuring that appropriate information is communicated to the media and external parties thereby safeguarding MDI NetworX's reputation and maintain consistency in the information released. Since the MMT has to deal with sensitive information, it will comprise of senior management personnel.

Key Tasks

#	Key Tasks	Liaison
1	**Assemble the team** • Liaise with external agencies such as Law firms, PR agencies etc. and assemble the team that would assist in managing communication. Apprise the team about the existing conditions based on communications received from the ERT and BSC.	• ERT • BSC • PR Agencies
2	**Drafting communication** • Create a draft of the intended media communication in association with the BSC. • Secure clearance from the LRMT for the intended communication.	• BSC • LRMT

#	Key Tasks	Liaison
	• Prepare appropriate press releases / communication for the senior management personnel periodically.	
3	**Liaise with the media** • Release official communication to the media. Publicize the contact information and emergency numbers of the contingency location which the external parties can contact for obtaining information. • Organize for a press conference / live coverage depending on the type and extent of disaster.	• PR Agencies
4	**Instructions to employees** • Ensure that all employees are instructed not to communicate directly with the media but to redirect all media enquiries to the MMT. • Inform the employees about the situation periodically.	• EST (Employee support Team)
5	**Formulate public relations plans** • Contact public relations agency to manage public relations. • Formulate strategies and campaigns to build public confidence by assuring them of MDI NetworX's capabilities to respond to disasters and the actions taken to ensure speedy resumption of normal business operations (depending upon the impact of the disaster).	• PR Agencies
6	**Activate communication channels** • Activate communication channels that have been set up for providing information to: – Business Partners; – Vendors; and – Employees	• ITRT • AST
7	**Website Update** MDI NetworX website is periodically updated to communicate the measures that MDI NetworX is taking to address the disaster situation and further provide emergency contact information.	• ITRT
8	**Monitor media** • Monitor media reports and issue clarifications wherever required. • Initiate appropriate legal action whenever required.	• LRMT
9	**Key stakeholder relationship** • Address key stakeholders through media communication to provide assurance about viability of MDI NetworX's business operations.	• Top management • All FRTs

9.5 Information Technology Recovery Team (ITRT)

Role

The Information Technology Recovery Team (ITRT) is responsible for assessing the possibility of using IT assets existing at the affected location. The ITRT is also responsible to ensure the availability of the critical business applications systems and IT infrastructure at the contingency location. The team will comprise of the key IT personnel.

Key Tasks

#	Key Tasks	Liaison
1	**Activate IT infrastructure at contingency location** • Make necessary configuration / networking changes to enable users to access the required business applications and connect to the outside world.	
2	**Information Dissemination** • Ascertain critical business processes/ functions that rely on the business application systems. • Determine the extent of reusability of critical IT resources. • Communicate to the FRTs of the availability/ non-availability of the relevant systems.	• SRT (Salvage Recovery Team) • AST • FRTs
3	**Contact third party service providers** • Contact third party service providers for setting up the IT infrastructure and ongoing support at the contingency location.	• Third party service providers
4	**IT Systems and data recovery** • Restore the critical business applications and hardware components. • Contact the offsite storage location (if different from the contingency location) and arrange for the latest backup tapes to be made available at the contingency location.	• Personnel at the offsite storage location (if any)
5	**Monitor Systems** • Monitor IT systems at the contingency location to ensure its security and availability, since IT security implemented at the contingency location may not meet the existing security settings.	
6	**Procure Additional IT infrastructure** • Ascertain whether capacity of the contingency location is adequate to meet the processing requirements, if not then commence the process for procuring additional IT infrastructure. • Facilitate the procurement of new hardware that has been damaged in the disaster.	• FST • SRT

9.6 Legal Risk Management Team (LRMT)

Role

Disruption of the business may hinder the organization's ability to deliver the committed level of services which may impact existing contractual obligation. This could have a severe impact on the organization's reputation, unless adequate safeguards have been initiated to ensure that the legal risk is properly managed. The Legal Risk Management Team (LRMT) will be responsible for identifying the legal issues and devise strategies to mitigate the same. The LRMT will comprise of senior officers from the legal department, functional heads and legal advisors.

Key Tasks

#	Key Tasks	Liaison
1	**Identify the likely areas of litigation** • Examine the checklist of agreements to ascertain probable areas which may impact existing contractual obligation. • Accordingly advise BSC, regarding possible financial and legal risk.	• BSC
2	**Review draft media communication** • Review the draft media communication prepared by MMT and BSC to ensure exclusion of any matter that might result in MDI NetworX facing litigation.	• BSC • MMT
3	**Liaise with MMT** • Liaise with MMT and BSC on a daily basis to prevent any potential litigation issues arising on account of: a) Inaccurate reports to the media b) Non-compliance of contractual obligations with business partners • Accompany BSC for meetings with key business partners or third parties, if and wherever required.	• BSC • MMT
4	**Liaise with legal advisors** • Secure legal advice from lawyers and take proactive legal measures. • Deliberate with legal counsel regarding enforcement of contracts/ obligations which warrant rendering services as stated in their agreement clauses.	• Legal advisors
5	**Liaise with regulatory authorities** • Obtain the necessary approvals/ concessions from regulatory bodies, if required.	• Regulatory Authorities

9.7 Employee Support Team (EST)

Role

In the event of a disaster the Employee Support Team (EST) will provide required support to employees and families of employees impacted by the disaster. It is advised that the team members receive formal training in crisis management and counselling. The EST will comprise of personnel from human resources department and functional departments.

Key Tasks

#	Key Tasks	Liaison
1	**Information Dissemination** • Contact the families of employees, whenever required, informing them about status of the respective employees. • If the situation demands as well as permits, visit the families of employees.	-
2	**Establish communication channel** • Co-ordinate with ITRT to set up a hotline for employees and the families of employees. • Ensure that correct information is disseminated. • The EST will be trained to converse in an encouraging and morale boosting manner. • Maintain open channels of communication with the employees to apprise them on the ongoing status of the employees affected in the disaster. • Update the BSC on important developments, and if required, facilitate meetings between BSC and the employees' families.	• Third party representatives
3	**Liaise with the Emergency Response Authorities** • Supplement the efforts of ERT in rendering medical attention to employees. • Maintain contact with the impacted employees on a regular basis and provide necessary support.	• ERT
4	**Assistance to employees / employees' families** • Provide necessary assistance to families of impacted employees such as filing of insurance claim, payment of hospital deposits, financial assistance etc. • If relocation of an employee is required, ensure that their families are also supported on issues such as admissions of children to schools, arrangement for dependent parents, etc.	• FST
5	**Organize Counselling** • Coordinate with counsellors for conducting counselling sessions for the disaster struck employees. • Organize events that will help in boosting the morale of employees.	• Counsellors
6	**Compensation Pay-outs** • Arrange for compensation and other such payments to be made to the employees by resolving the same with the BSC.	• BSC • FST
7	**Liaise with Regulatory Authorities** • Ensure timely release of dues to the affected employees by coordinating with regulatory agencies such as Provident Fund Authorities, Death Certifying Authorities, etc.	• Regulatory Authorities

#	Key Tasks	Liaison
8	**Facilitate emergency recruitment and training** • Assist the BSC and FRTs in case of emergency recruitment to fill vacancies created due to employees impacted by the disaster. • Gather information regarding urgent training needs from FRTs and organize training programs.	• BSC • FRT

9.8 Finance Support Team (FST)

Role

The Finance Support Team (FST) will be responsible for estimating the fund requirements and the speedy disbursement of funds to the Business Continuity Teams and FRTs, as and when required during the recovery operations. The FST will comprise of personnel from the finance and human resources departments.

Key Tasks

#	Key Tasks	Liaison
1	**Liaise with bankers of MDI NetworX** • Assess the financial position of MDI NetworX by contacting their bankers. • Notify the bank about the change in signatories, wherever required.	• Banks
2	**Estimating fund requirements** • Obtain a primary estimate of funds required by each Business Continuity Teams and FRT. The estimate will also provide justification for funds required.	• Business Continuity Team • FRTs
3	**Arrange for Funds** • Ascertain requirement for additional funds based on net position of funds; accordingly consult with BSC for arranging the same. • Obtain internal approvals, if required. • Distribute adequate cash advances to the Business Continuity Team and FRTs. Ensure that there is not much variance in estimated fund requirements and the disbursed amounts.	• BSC • Business Continuity Team • FRTs
4	**Advances in lieu of salary** • Procure a list of employees and disburse advances in the event formal salary payments are not being made. • Ensure adequate records are maintained for the same.	• EST • FRTs
5	**Liaise with the Business Continuity Team** • Obtain expense reports with supporting vouchers from Business Continuity Team. • Record all financial transactions regarding the recovery operations separately.	• Business Continuity Teams

#	Key Tasks	Liaison
7.	**Obtain information on fixed expenses** • Obtain list of monthly payments to be paid along with the due dates. • As far as possible, ensure that payment of statutory dues such as Provident Fund, Employee State Insurance Contribution, etc. is not delayed.	• Regulatory Authorities • EST
8.	**Liaise with BSC** • Update BSC on a daily basis on the funds position of MDI NetworX.	• BSC

9.9 Administration Support Team (AST)

Role

The Administration Support Team (AST) will play an important role and will be responsible to ensure that the relevant administrative functions are triggered post the disaster to facilitate the movement of people and resources to the designated contingency locations. The AST will comprise of personnel from the administration department.

Key Tasks

#	Key Tasks	Liaison
1	**Relocation of employees** • Arrange for transportation of the identified Business Continuity Teams and FRT members to the contingency location. • Arrange for accommodation for the team members. • Follow the recommended procedures for relocating the personnel at the contingency location.	• Travel Agents • Hotels
2	**Restoration of resources** • Arrange for transportation of resources that have been salvaged based on information provided by the SRT. • Facilitate the repair of assets that can be salvaged by contacting relevant service providers. • Make necessary arrangements to move all repaired assets to the respective contingency locations based on minimum infrastructure requirements at these locations.	• SRT • ITRT
3	**Activation of Basic Facilities** • Facilitate the activation of identified facilities at the contingency location such as: – Telephone (call forwarding from affected location) – Security Arrangements – Other facilities as maybe required	• FRTs
4	**Facilitate procurement and allocation of equipment** • Facilitate the replacement of assets that have been destroyed beyond repair by receiving approved recovery resource requests from the FST and providing vendor delivery instructions.	• FST • Business Continuity Teams

#	Key Tasks	Liaison
	• Ensure that the purchased resources are distributed to the appropriate Business Continuity Teams.	
5	**Clean up of affected location** • Devise appropriate strategies for removal of non-restorable items from the affected location. • Assist BSC in restoring the affected site. • Facilitate the movement of employees and resources from contingency location after restoration activities have been completed at the affected location.	• SRT • BSC • ITRT • Structural Engineers
6	**Collating information** • Co-ordinate with the relevant travel authorities such as Airports, Indian Railways, Traffic Department, etc., for latest update and accordingly inform BSC, Business Continuity Teams and FRTs.	• BSC • Business Continuity Teams • Travel Agents • Travel Authorities

9.10 Function Recovery Teams (FRTs)

The Function Recovery teams (FRTs) will consist of leaders from various departments who will assist the Business Continuity Teams in the process of relocation to contingency location. The main responsibility of function recovery teams is to ensure that critical processes are resumed at the contingency location within the RTO defined in the Business Continuity Plan. The composition of the function recovery team may vary according to the size of the process. Please refer FRT annexure for specific resource recovery requirement for critical processes along-with FRT details.

Escalation tree for Function Recovery Team

The Processes have been identified for allocation of Function Recovery Teams:

Key Tasks

#	Key Tasks	Liaison
1	**Gather Information** Liaise with the ERT to identify the personnel from the respective processes who have been affected by the disaster. **Action Steps** • Acquire information from ERT or other key personnel at the affected location. • Obtain information from the BSC and AST about the plans for relocation. • Identify the personnel who have to report in the next shift and obtain information from BSC about the instructions to be given to them. • Liaise with ITRT to ensure that necessary infrastructure has been set up for resumption of operations at contingency location	• ERT • Key personnel at the affected location • BSC
2	**Disseminate Information** Liaise with the practice heads to identify the personnel to be transported to the contingency location. **Action Steps** • Liaise with other FRTs to finalise the order of prioritization in which the personnel will be transported to contingency location • Inform the AST about the details of the personnel to be transported to the contingency location. • Inform the ITRT about the tentative time of resuming operations from contingency location and the prioritization order for the same.	-
3	**Invoke Call Tree** Ensure that all associates are aware of the occurrence of a disaster and instructed of the course of action to be followed. **Action Steps** • Invoke call tree to disseminate the message, “a local or regional disaster has occurred impacting associates’” throughout the communication chain.	-
4	**Coordinate resumption activities** Ensure that the resumption procedures at the contingency location are proceeding as per the Recovery Time Objectives defined in the Business Continuity Plan. **Action Steps** • Liaise with the identified contacts at alternate site to ascertain the progress of resumption activities at contingency location. • Escalate any disruptions in resumption procedures to the Practice Head and BSC and apprise them of the progress from time to time.	-

10 Incident Management Plan Emergency Response Plan

10.1 Emergency Response Plan

10.1.1 Invocation of a disaster

The BCP will be invoked for onsite recovery or offsite recovery depending on the type of disaster situation. Once an incident has been declared a disaster, the plan, roles and responsibilities remain in effect until the incident is resolved and authorities are notified. Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable recovery support has been established.

10.1.2 Escalation procedures

On identification of an emergency situation involving disruption of business processes / IT systems, the following information will be conveyed to the ERT Leader immediately by any of the Recovery Team Member:

- Nature of the emergency
- Location of the emergency
- The time when the emergency was identified
- Any casualties

10.1.3 Employee Calling Tree

The Emergency Response Team (ERT) Leader will utilize the Employee Calling Tree in order to ensure that all employees are contacted and informed that a disaster has been declared as per the flow chart below:

The following format will be used for 'employee calling tree':

- When a call notifying a disaster is received, the personnel is required to write down the received message and read it back to the caller to verify its accuracy.
- The message should be read to each person called, briefly stating the nature of the problem. Speculation on injuries or damage should not be made to avoid possible confusion among employees.
- Making comments to press, news media, outside customers, vendors, etc. should be avoided. An official management designated spokesman will only provide the news release to the press, news media, etc.
- Give instructions to each contacted individual as to what she/ he is expected to do (i.e., report to the recovery location and standby for further instructions). The Team Leader will activate only the recovery team members needed immediately and prepare a work schedule for others.
- Make a record of all calls and report the notification results to the management team.
- The initial attempts to contact the recovery team members should not exceed two hours. After that time, the Team Leaders will list the names of individuals they were unable to contact and assign someone to continue the notification.
- For the detailed responsibility matrix for key activities to be performed by each recovery team member in the event of a disaster is mentioned in the annexure recovery team details (submitted separately).

The initial attempts to contact the recovery team members should not exceed two hours. After that time, the Team Leaders will list the names of individuals they were unable to contact and assign someone to continue the notification.

10.1.4 Assembly Area

Assembly area is the safe area identified by MDI NetworX outside the premises for all personnel to assemble in the event of a disaster. After the members have been released from the initial emergency assembly, all members shall meet together to determine the status of each member in order to get an accurate headcount and assess the impact to the organization.

Instructions for all Critical resources:

- Ensure that your contact numbers are up to date with your reporting supervisor; In case of any changes in your contact details ensure that the same has been updated.
- Be well aware of your role in case of an incident. Probe your reporting managers for any kind of clarification if required regarding your role during an incident.
- Listen to the instructions given by the CIMT members and adhere to them.
- Be reachable on your mobile number.
- Do not keep your phone engaged for an unnecessary period of time. Activate call waiting facility on your cell phones.
- Co-operate with the CIMT members.
- Since you are the part of the critical resources team from your department be vigilant of the happenings around you and be ready to extend your support to the team.

Instructions for all Non- Critical resources:

- Ensure that your contact numbers are up to date with your reporting supervisor; In case of any changes in your contact details ensure that the same has been updated.
- Be well aware of your role in case of an incident. Probe your reporting managers for any kind of clarification if required regarding your role during an incident.
- Listen to the instructions given by the CIMT members and adhere to them.
- During an incident if you are instructed to leave for home, ensure that you safely reach home.
- Ensure that you are reachable over your mobile phone for the CIMT members/Other team members, as they may need to communicate to you the further instructions (If any).

10.1.5 Command centre

In the event of a disaster at MDI NetworX business premises, a command center will be established. All activities associated with the restoration of the critical business processes at the affected premises will be coordinated from the command center.
The command center will be used by the ERT to coordinate all recovery efforts. MDI NetworX will have an identified command center. The command center may require some of the following resources:

- A room where the Recovery Team Members can sit together and discuss issues related to the disaster
- Telecommunication lines for access
- Fax machine
- A copy of BCP document
- A copy of Recovery Team Details.
- One PC with basic software e.g. MS Office, anti-virus, etc.
- A printer
- Basic stationery - pens, pencils, writing pads, A4 size papers, company letter heads, company envelopes, visiting cards, etc.

The designated command centre depends on the scale and nature of disaster:

10.2 Disaster declaration

A preliminary announcement will be used to communicate, responsively and accurately, to MDI NetworX employees immediately following the disaster.

BCM Committee, with input from the ERT and BCP Coordinators, will develop and document a preliminary announcement. The disaster declaration announcement to employees should include the following, at a minimum:

- Initial assessment of the problem.
- Extent of damage and possible cause (if known).
- Where and how employees should direct questions and/or problems.
- Time of intimation of additional information regarding the disaster.

11 Awareness Training and BCP testing

11.1 BCP Awareness Training

MDI NetworX BCM Education and Awareness Program should be, but are not limited to:

- Training management in the concepts of Business Continuity Management and Disaster Recovery
- Training management in the concepts of Business Continuity Plan Exercising, Maintenance, and Distribution
- Highlighting to all the business benefits of Business Continuity Management and Disaster Recovery
- Maintaining a constant state of readiness for Business Owners and key employees who are required to assist in recoveries
- Training those who will be affected by business interruptions of their communication process and responsibilities
- Briefing investors in the reliability of MDI NetworX's recovery procedures
- Heightening the awareness of the program for all employees, whether directly or indirectly involved in maintaining and/or executing the plan

Awareness is the need for maintaining a viable recovery capability is essential. This awareness will be achieved through formal education and training sessions that will be conducted annually. All employees of MDI NetworX will be trained in basic 'Dos and Don'ts' procedures such as emergency evacuation, safety precautions for Fire, earthquakes and other environmental / man-made emergency situations, etc. during induction.

The objective of the training is to:

- Ensure that all the personnel who are responsible for maintaining and executing the plan have necessary awareness and understanding of the Business Continuity procedures.
- Train key personnel to keep the Business Continuity plan updated.
- Increase Business Continuity planning awareness for those personnel who are not directly involved in maintenance and/or execution of the plan.

11.2 BCP Testing

Annual review and updating of the Business Continuity plan will ensure that the information contained within the plan is current. The testing of the plan will determine:

- The state of readiness of the business to respond to and cope with a disaster involving the IT systems as well as facilities.
- Whether backup of data and documentation stored at offsite are adequate to support the recovery of IT systems.
- Whether the defined tasks and procedures are adequate to support the recovery of business processes / IT systems within the given time frame.
- Whether the Business Continuity plan has been properly maintained and updated to reflect the current status.

11.2.1 Types of Tests

Structured walkthrough

Also referred to as a "table-top" exercise, the structured walkthrough is a paper evaluation of BCP designed to expose errors or omissions without incurring the level of planning and expenses associated with performing an operations test. In the structured walkthrough, a disaster scenario is established, and recovery teams assemble in a conference room and walkthrough their recovery actions.

A scenario will be made available in advance to allow the recovery team members to review their recovery actions in response to the test scenario. At the end of the structured walkthrough any changes to the plan that are found to be necessary will be documented and implemented.

Component testing

Component tests are actual physical exercises designed to assess the readiness and effectiveness of discrete plan elements and recovery activities. The isolation of key recovery activities allows recovery team members to focus their efforts while limiting testing expense and resources. This testing is effective for identifying and resolving issues that may adversely affect the successful completion of a full operations test. Component tests include:

- Evacuation tests.
- Emergency notification test.
- Backup restoration test.
- Business application recovery test.
- Remote or dial-in access test.
- Manual Workaround for a process

Full interruption test

The full interruption test requires extensive planning and preparation and should not be performed until most, if not all, of the plan components have been tested. This test requires the simulated recovery of critical business application systems and communication components. It is the closest exercise to an actual disaster scenario. Although a full interruption test requires weeks of planning and considerable coordination of personnel and resources, the exercise provides highest level of confidence about the ability to recover in an actual event.

11.2.2 Frequency of testing

The following table provides frequency for carrying out various types of tests in order to keep the Business Continuity plan current and maintain the efficiency of the recovery teams. While proposed frequency of testing has been included in the table below, changes can be made with the approval of Chief Recovery Officer (CRO).

Type of tests	Frequency of the test		
	Quarterly	Six Monthly	Yearly
Structured Walkthrough	✓		✓
Component Testing		✓	
Full Interruption Testing			✓

11.2.3 BCMS Internal Audit

MDI NetworX shall ensure that internal audit of the BCMS is conducted on a periodic basis to determine whether the BCMS:

- Conforms to planned arrangements for BCM, including the requirements of the ISO22301:2019 standard
- Has been properly implemented and is maintained
- Is effective in meeting the BCM policy and objectives as documented in the BCMS manual
- Provide information on the results of the internal audits to the management

MDI NetworX's management has laid down an internal audit program for all the functions.

12 Maintenance Plan for BCP

12.1 BCP Governance Procedures

The BCP is a live document, and most sections of this document require up to date information. Therefore, the BCP needs to be reviewed and updated on a regular basis. MDI NetworX will ensure that a formal governance process is incorporated to keep the document updated.

12.2 BCM Manager

- BCM Manager will have overall responsibility for maintaining this document up to date and he will be owner of this document.
- He/she will be responsible for the maintenance, review and update of this document.
- He/she will be responsible for coordinating the review of this document with all Business Continuity Teams and Function Recovery Teams (FRTs) that are involved in the BCP process.
- He/she will be the liaison between the Business Continuity Teams and FRTs and the BCP Steering Committee.
- It is his/her responsibility to ensure that Business Continuity Teams and FRTs meet on a monthly basis individually and on a quarterly basis collectively.
- He/she will act upon the actionable items raised out of these meetings.
- When a new version of the document is prepared, he/she will make sure all old copies are replaced and distributed.

12.3 Procedures for administration of the plan

The objective of developing procedures for administration of the Business Continuity plan is to keep the plan updated by promptly processing the changes necessary for maintaining a workable Business Continuity plan. Specific plan administration activities ensure that the plan is updated and include:

- Updating of the Business Continuity plan by the Recovery Coordinator.
- Developing administrative procedures to control changes within the Business Continuity plan and controlling distribution of the plan.
- Providing the necessary standards and procedures, which ensure compliance with plan requirements.
- Developing a training program to include all executive management, recovery teams and the user community.
- Instituting procedures for planning, developing, scheduling, and executing tests of the Business Continuity plan including the evaluation of test results.
- Assisting internal audit in the performance of compliance audits, to ensure overall compliance with recovery plan administration procedures that provide assurance on the viability, accuracy, and currency of the Business Continuity plan.
- Maintaining the Business Continuity plan in electronic format for ease of maintenance.

12.4 Competency of BCM Personnel

The Business Continuity Coordinator along with the HR team ensures that all the BCM resources who are assigned BCMS responsibilities are competent to perform the required tasks by:

- Identifying the competencies required for performing the BCMS tasks
- Undertaking a training needs analysis
- Providing necessary trainings or hiring people with required competencies to manage the BCMS program

- Evaluating the effectiveness of the training provided

Competency required for effective execution of all roles and responsibilities within BCMS are defined and documented in the BCMS Governance procedure.

12.5 Meeting Procedures

- BCM Manager will be the main facilitator of all the meetings in relation to BCP.
- Individual Business Continuity Teams and FRTs will meet on a monthly basis to review their team composition, key tasks and any changes that need to be incorporated.
- All Business Continuity Teams will meet together on a quarterly basis to review each other's tasks and bring out any concerns on the BCP.
- A detailed agenda will be prepared prior to the meeting. The typical agenda for BCP meetings will include, but not limited to:
  - Resolution of action points from previous meetings
  - BCP governance updates e.g. Training and Testing
  - Resolution of control gap analysis
  - Process changes
  - Infrastructure changes
  - Changes in operation teams and support function composition
  - Changes in Business Continuity Teams and FRTs
  - Updating the information contained in BCP annexure
- Minutes of the meeting will be recorded and distributed by BCM Steering committee leader, who will monitor the actionable items.

12.6 Corrective/Preventive action

Corrective/ preventive action shall be documented using the CAPA (Preventive and Corrective Action) form, if following are observed:

- Learning's from any incident
- Post BCMS exercises planned as part of the program
- Post self-assessment reviews
- Non-conformities received after internal and external audits
- Post management review of BCMS
- Non-conformities received after third party/internal audits

Detailed process, roles and responsibilities for maintaining and improving the BCMS arrangements are defined and documented in the BCMS PACA procedure.

12.7 Update Triggers

Business is driven by People, Processes and Technology / Infrastructure. Any change to these factors will warrant changes to the BCP. Every business has some information that is static and some information that is dynamic. The dynamic information forms a part of the update triggers in the BCP.

Various standardised templates have been developed for collating information from various areas of the business. The responsible team members will use these templates to update information in the BCP, which in turn will be analysed to update various sections of the BCP.

13 Distribution of the plan

13.1 Introduction

BCP is a confidential document as it contains proprietary information. For the purpose of this plan, confidential information is defined as the information that could have an impact on MDI NetworX (MDI NetworX or the company) or its stakeholders, which if available to unauthorized parties, for example is be valuable to external parties/competitors. The information contained in this document is non-public information rightfully obtained, developed and produced by or on behalf of MDI NetworX and/or its employees for the benefit of MDI NetworX. The information contained in this document is owned by MDI NetworX.

This document has been classified as Confidential and is for restricted distribution only, as it contains MDI NetworX's strategy for recovery of critical business processes / IT systems in the event of a disaster, and names, addresses and telephone numbers of the recovery team members. Therefore, the plan should be distributed on a need-to-know basis within the organization only.

Each individual possessing a copy of the BCP is responsible for security and control of the document in accordance with the policies for the protection of proprietary information.

13.2 Responsibility

The BC Manager/ BC Steering Committee is responsible for the authorized distribution of the Business Continuity plan. This is accomplished by developing a master distribution list on a need-to-know basis.

13.3 Review, Approval and Distribution

The BCP will be reviewed for completeness and correctness of the information included in it, once a month. The review process will cover generic as well as dynamic information.

The BCP will be maintained and updated to reflect any changes to the operating environment, such as changes in:

- IT infrastructure
- Processes
- Human resource changes
- Location or arrangements at the primary or recovery site
- Service Level Agreement with the vendors, suppliers etc.

As part of this review, the BCM Manager and his/her team will audit the documented processes and make appropriate updates. Action plans will be developed if deficiencies are found, and this document will be updated to reflect the corrections. Each action item will have corresponding personnel responsible for carrying out that task along with timelines.

This document, on change, shall be subject to approval by BCP steering committee. The change shall be approved by respective practice heads / Business Continuity Teams leaders (as applicable) before their inclusion in the plan.

The distribution list for BCP document and its annexure will include all the BCP Steering Committee, Practice Heads and Business Continuity Teams. After every change in the plan and its annexure, BCM Manager will provide updated version of document to each member in the BCP distribution list.

14 Acronym Usage in BCP document

The BCP document and its annexure contain acronyms which are defined at the time of their first time usage in the document. However, the important terms (acronyms) are expanded in the table below for easy reference:

Acronym	Expanded
AST	Administration Support Team
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BSC	BCM Steering Committee
EST	Employee Support Team (HR Team)
FRT	Function Recovery Team
FST	Finance Support Team
ERT	Emergency Response Team
ITRT	Information Technology Recovery Team
LRMT	Legal Risk Management Team
LAN	Local Area Network
MMT	Media Management Team
RTO	Recovery Time Objective
SRT	Salvage Recovery Team

15 Annexures

Following is the list of annexures that have been referenced in the various sections of this document:

15.1 Emergency Contact Details


Emergency Contact Details.xlsx

15.2 Employees Do's and Don'ts


Employee's Do's & Don'ts.doc

15.3 First Aid Measures


First Aid Measures.docx

15.4 Communication


Disaster Communication Tem

15.5 Assembly Roll Call Sheet Template


Roll Call Sheet.xls

15.6 Damage Assessment Form


Damage Assessment Form.dc

15.7 IT Request Form

https://servicedesk.mdinetworx.com/

15.8 Continuity Test Template

BCP Test Report.docx

15.9 Work From Home

GRC014-Work From Home Policy.pdf

15.10 BCM Team Composition

Acronym	Expanded	Team Composition	People Recommended (not mandatory)	Details of Team Members
BSC	BCM Steering Committee	BSC will comprise heads of departments and senior management personnel.	8 to 10 personnel	Team Contact Details.xlsx
ERT	Emergency Response Team	The ERT comprises mainly the administrative personnel and is led by a representative from the administration department and vendor security teams.	8 to 10 personnel	
AST	Administration Support Team	The AST will comprise personnel from the administration department.	3 to 5 personnel	
EST	Employee Support Team (HR Team)	The EST will comprise personnel from human resources department.	2 to 4 personnel	
FRT	Function Recovery Team	The composition of the function recovery team may vary according to the size of the department.	2 to 3 personnel per department.	
FST	Finance Support Team	The FST will comprise personnel from the finance and human resources departments.	2 to 3 personnel	
ITRT	Information Technology Recovery Team	The team will comprise the key IT personnel.	1 to 2 personnel	

Acronym	Expanded	Team Composition	People Recommended (not mandatory)	Details of Team Members
LRMT	Legal Risk Management Team	The LRMT will comprise of senior officers from the legal department, functional heads and legal advisors.	1 to 2 personnel	
MMT	Media Management Team	MMT has to deal with sensitive information, it will comprise of senior management personnel.	2 to 3 personnel	
SRT	Salvage Recovery Team	Comprises mainly of the administrative personnel	2 to 3 personnel	

15.11 Command Centre

15.11.1 Physical Command Centre

The primary location of Command centre (CC) should be the primary location of the BCM Committee, and the alternate CC should be a safe distance from the main office location, but it shall be within the same city as the primary office (in the same city where BCM Committee members reside).

Sr. No	Command Centre Location	Address
1.	Primary Location	Primary Center: 8717 West 110th St, Ste 480 Overland Park, KS 66210
2.	Secondary Location	Secondary Center: 717 East Ordnance Road, STE 208 Baltimore, MD 21226
3.	Alternate Location	Backup Center: AWS, US East coast (N.Virginia)

15.11.2 Virtual Command Centre - Conference Bridge

In the event when command centre at the mentioned physical location is not accessible or if an event occurs after normal working hours, the BCM Committee should convene virtually via following any of the convenience conference bridges.