



DISASTER MANAGEMENT PLAN

STATE ELECTRONICS DEVELOPMENT CORPORATION

GOVERNMENT OF HIMACHAL PRADESH

Contents

Chapter 1 - Introduction	04
1.1 Overview of the Department	04
1.2 Purpose of the Plan	05
1.3 Scope of the Plan	05
1.4 Authorities Codes Policies	06
1.5 Institutional Arrangements for Disaster Management	06
1.6 Plan Management (Monitoring Review and Revision)	07
1.7 Dissemination of Plan	07
Chapter 2 - Hazard Risk and Vulnerability Analysis	08
2.1 Risk Assessment of Himachal Pradesh	08
2.2 Assessment of Sectoral and Department Risks	08
Chapter 3 - Risk Prevention and Mitigation	10
3.1 Risk Prevention	10

Chapter 4 - Disaster Preparedness	14
4.1 Strategies for Disaster Preparedness	14
4.2 Measures for Disaster Preparedness	14
Chapter 5 - Disaster Response and Recovery	17
5.1 Disaster Recovery Plan and Business Con- tinuity	17
5.2 Disaster Recovery Plan Criteria	18
5.3 DR Team - Roles and Responsibilities	18
5.4 Contingency Procedures	18
5.5 Testing and Maintenance	19
5.6 Roles and Responsibilities of the Nodal Officers	19
Chapter 6 - Financial Resources for Implementation of DMP	21

Chapter-1: Introduction

1.1 Overview of the Department

Himachal Pradesh State Electronic Development Corporation Ltd (HPSEDC) was incorporated under the companies Act 1956 in the year 1984.

The main objectives and functions of this Corporation include promotion of Computerization in the State (particularly in the State Government Departments and its undertakings), development of software packages, procurement and supply of computer hardware, software and other related electronic products, office automation and medical equipments at reasonable rates. HPSEDC also undertakes site preparation works for computer installations, networking solutions, data processing, and providing technical consultancy. In addition to this the corporation is expected to give fillip to electronic and IT industry in the state by developing adequate infrastructure.

To promote, establish, run, manage, execute, administer, supervise, finance, advise, improve, assist and to develop and operate schemes including investment, financial and electronics with or without government aid/ assistance and with or without foreign collaboration, and for the purpose to prepare and or cause to be prepared investigations and statistics and other relevant information and to provide consultancy services for the establish companies, subsidiary or other-wise and associations for setting up industries in the line of production which are important in the opinion of the Corporation for the development of Electronics and Electrical industries.

The major activities of the corporation can broadly be categorized into the following areas:

1. Consultancy and Promotional Services related to development of Electronics and IT's in the State.
2. Software Development and Computerization on turn-key solution by providing optimum computer hardware / software's and other peripherals.
3. Procurement & Marketing of All types of Electronic Office Automation including Medical and Pollution control products.
4. Development of Industrial Buildings/ Sheds and Areas.
5. To provide prompt after - sales - support / services for the supplied / installed Electronics items by the Corporation to the concerned users departments.

1.2 Purpose of the Plan

Need for disaster management plan for Forensic Medicine expert so that Medical officers and Forensic expert can efficiently work during mass disaster. There are certain fundamental principles which should be thoroughly understood by everyone who may have responsibility for helping the victim of a disaster, it is important that these principles be applied in the proper sequence; otherwise they lose effectiveness or cause even more deaths and injuries.

When a mass fatality incident occurs, identifying the bodies is an intensive and, in some cases, time consuming process, which is often perceived as taking too long by the surviving relatives. In most cases it is not the recovery of the bodies and recording their description that takes so long. It can often take much more time to obtain and collect the ante mortem information needed to identify the victim, especially if that information has to come from abroad.

A lack of understanding of the international procedures used to identify victims and the time the identification process, can often lead to dissatisfaction amongst surviving relatives and the relevant authorities regarding the speed of the identification process.

Following a mass fatality incident partnership between the countries is of paramount importance. The identification process can be expedited by prompt consultation between the representatives of the countries involved, with consideration to the magnitude of the disaster and an understanding of the Disaster Victim Identification (DVI) process itself.

Local authorities, also the relevant diplomats of the affected countries can play a vital role in alleviating the suffering of surviving relatives by communicating clearly and specifically regarding the situation and events, as well as the progress of the investigation.

1.3 Scope of the Plan

In accordance with the Disaster Management Act 2005 and Himachal Pradesh State Disaster Management Plan 2012, the plan must include the following:

- Identify the vulnerability of different parts of the State to different forms of disasters in context of the department;
- The measures to be adopted for prevention and mitigation of disasters;

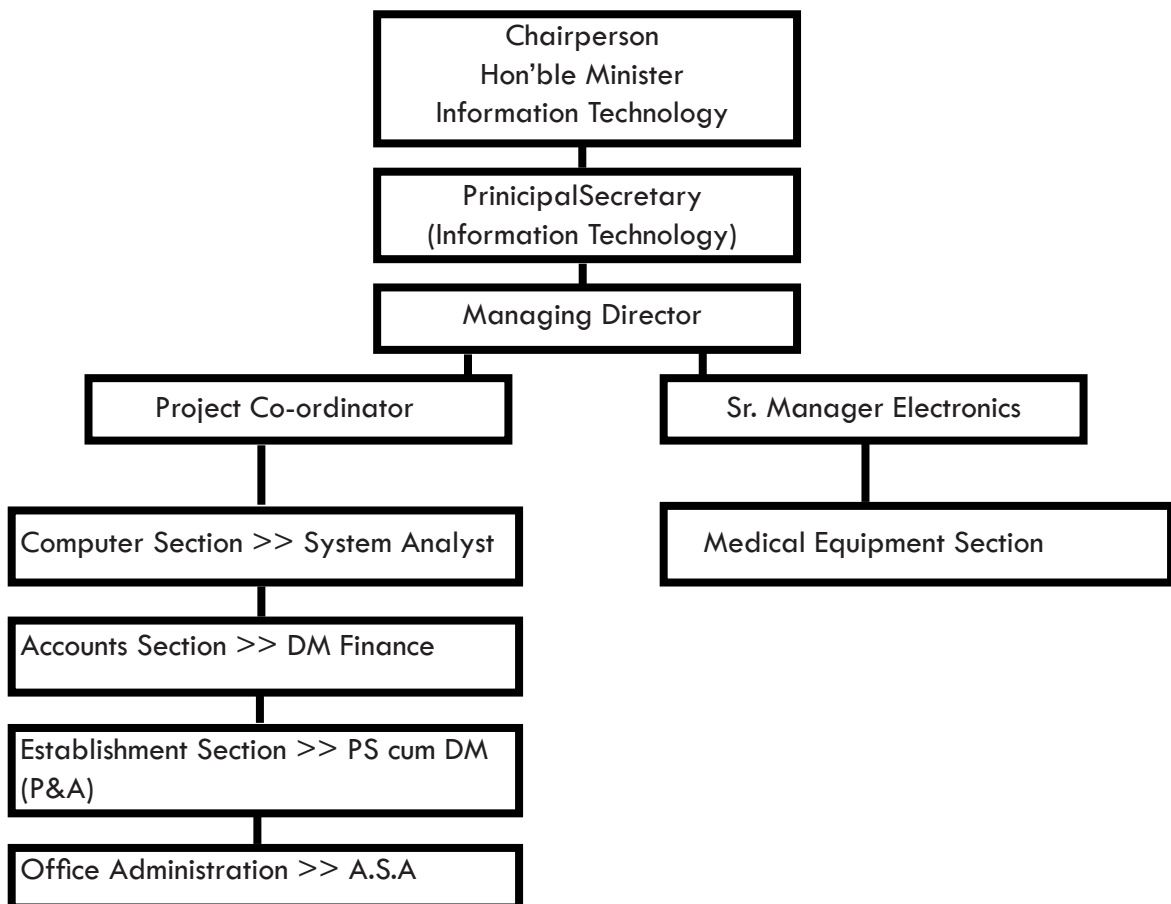
- The manner in which the mitigation measures shall be integrated with the development plan and projects;
- The capacity-building and preparedness measures to be taken;
- The roles and responsibilities of different departments of the Government of the State in responding to any threatening disaster situation or disaster;

1.4 Authorities, Codes, Policies:

Section 40 of the Disaster Management Act 2005 provides that there shall be a Disaster Management Plan for every Department of the State. The departmental DM Plan shall be prepared by each department and shall be approved by the State Executive Committee. This plan is prepared under the provisions outlined in the Disaster Management Act 2005.

1.5 Institutional arrangements for Disaster Management:

Organogram of HPSEDC



1.6 Plan Management (Monitoring, Review and Revision):

DM Plan is a “Living document” and would require regular improvement and updating. The plan must be updated at least once a year. The Disaster Management plan prepared by the Department shall be circulated to all its district offices. The Plan shall be shared on the Departmental portal. The plan will be updated as and when required and modified plan shall be communicated to the key stake holders.

For the annual review of the disaster management plan participation of different stakeholders will be ensured by inviting them to workshops. Based on their feedback, necessary changes will be incorporated in the plan.

1.7 Dissemination of Plan

The primary responsibility for dissemination of the plan will be with the HPSEDC. They would involve HPSDMA for capacity building at different levels for training and dissemination. The Disaster Management Plan will be disseminated at three levels: District authorities, government departments, hospitals/ health centers and other agencies and institutions within the State. The content of the plan would be explained through well designed and focussed awareness programmes. The awareness programmes would be prepared in the local language to ensure widespread dissemination up to the school level. Disaster Management Plan will be uploaded in the department website of department. A printed document will be supplied to all the stakeholders.

Chapter-2: Hazard, Risk and Vulnerability Analysis

2.1 Risk Assessment of Himachal Pradesh

The state of Himachal Pradesh is exposed to a range of natural, environmental and man-made hazards. Main hazards consist of earthquakes, landslides, flash floods, snow storms, avalanches, GLOF, droughts, dam failures, fires, forest fire, lightning etc. Enormous economic losses caused due to natural disasters such as earthquakes, floods, landslide, avalanche, etc., erode the development gain and bring back economy a few years ago. Most of the fatalities and economic losses occur due to the poor construction practices, lack of earthquake resistant features of the buildings and low awareness about disasters among people. In order to estimate and quantify risk, it is necessary to carry out the vulnerability assessment of the existing building stocks and lifeline infrastructure.

The entire state is at risk of being affected by a severe seismic event. About 32% of the total geographical area of Himachal Pradesh falls in the very high seismic zone V, while the rest (68%) lies in the high seismic zone IV. Ten out of 12 districts fall in the very high seismic zone. Three districts have over 90% of their geographical area prone to very high seismicity. Two districts have more than 50% of the geographical area with the severest seismic intensity: Chamba (53.2%), and Kullu (53.1%). During 1800–2008, about 70% of earthquakes occurred in three districts, namely, Chamba, Lahul and Spiti, and Kinnaur. Three districts, Solan, Hamirpur and Bilaspur, have less than 1% concentration, whereas in Una district, no earthquake has ever been recorded during this period but that doesn't mean that in future there will be no such events. In recent past the state has been facing mild earthquakes within short span which itself embarks the risk and gives the scope to assess it for mitigation.

2.2 Assessment of Sectoral and Departmental Risks

Organizations & Departments are adopting technology and standards to keep their IT infrastructure sound and to ensure business continuity. The continued operations of an Enterprise is determined by its ability to deal with potential natural or man-made disasters through creating an effective IT Disaster Recovery Plan (DRP) that can enable minimizing disruptions to the networks, and quickly restore normalcy of operations.

An IT Disaster Recovery Plan is a comprehensive documentation of well-planned actions that are to be

adopted before, during, and after a catastrophic event. In order to ensure business continuity and availability of critical resources during disasters, the plan should be documented and also tested in advance. This will help expedite the process when the actual disaster or emergency strikes. The key to IT or network disaster recovery is preparedness. The DR plan is the master tool of IT-based as well as other organizations to protect their IT infrastructure, ascertain organizational stability, and systematic disaster recovery. The primary objectives of IT/network disaster recovery planning include:

- Minimizing disruption of business operations
- Minimizing risk of delays
- Ensuring a level of security
- Assuring reliable backup systems
- Aiding in restoration of operations with speed

Business vulnerabilities are ever increasing and every organization is compelled to make appropriate disaster plans and use advanced technology to keep its network secure and stable. Network-reliant companies find it an absolute necessity to frame disaster recovery policies and procedures to respond to the varied circumstances and problems. In any organization that prepares itself for Disaster Recovery, the three main points to be considered are Prevention, Anticipation, and Mitigation. Prevention is the act of avoiding those disasters that can be prevented. Anticipation is to plan and develop adequate measures to counter unavoidable disasters. Mitigation is to effectively manage the disasters, and thereby minimize the negative impact.

IT Disaster Recovery planning involves a thorough analysis of existing network structure, applications, databases, equipment, organization setup, and related details. It is important to define in the document about the key components involved in the business, the disaster recovery team personnel with contact details, recovery time objective, and communication methods at the time of the disaster, alternative facility for the organization, and master list of all inventory, storage locations, customer/vendor, forms and policies. The following are the steps that should be taken in IT disaster recovery planning:

1. **Constitute a Disaster Recovery Team:** The organization should form a DR team that will assist in the entire disaster recovery operations. The team should be composed of core members from all departments with representative from the top management. The team will also be responsible for overseeing the development and implementation of the DR plan.
2. **Perform Risk Assessment:** A risk analysis and business impact analysis should be conducted, which includes in scope the possible disasters, both natural and manmade. By conducting an analysis of the impact and aftermath in disaster scenarios, the security of crucial resources can be determined.

3. **Prioritize Processes and Operations:** The organization's critical requirements pertaining to each department must be determined with respect to data, documentation, services, processes, operations, vital resources, and policies/procedures. They should all be categorized and ordered based on priority as Essential, Important, and Non-essential.

4. **Data Collection:** The complete data about the organization must be gathered and documented. It should include inventory of forms, policies, equipment, communications; important telephone numbers, contact details, and customer details; equipment, systems, applications and resources description; onsite and offsite location; details of backup storage facility and retention schedules; and other material and documentation.

5. **Creating the Disaster Recovery Plan:** The DR plan should be created in a standard format that would enable detailing of procedures and including essential information. All important procedures should be completely outlined and explained in the plan. The plan should have step-by-step details of what is to be done when the disaster strikes. It should also comprise procedures for maintaining and updating of the plan, with regular review by the Disaster Recovery team and top personnel of the organization.

6. **Testing the Plan:** The developed Disaster Recovery Plan should be tested for efficiency. Testing provides a platform wherein an analysis can be done as to what changes are required and make appropriate adjustments to the plan. The plan can be tested using different types of tests such as Checklist tests, Simulation tests, Parallel tests, Full interruption tests, etc.

Developing a good IT disaster recovery plan will enable organizations to minimize potential economic loss and disruption to operations in the face of a disaster. It will aid in organized form of recovery, ensuring that the assets of the organization are secure, and pave way for business continuity in the most resourceful manner.

Chapter-3: Risk Prevention and Mitigation

3.1 Risk Prevention

Most of the fatalities and economic losses occur due to the poor construction practices, lack of earthquake resistant features of the buildings and low awareness about disasters among people. In order to estimate and quantify risk, it is necessary to carry out the vulnerability assessment of the existing building stocks and other infrastructure.

Building Vulnerability assessment is carried out in three stages i.e. Rapid Visual Screening (RVS), Preliminary Vulnerability assessment (PVA) and Detailed Vulnerability Assessment (DVA). As detailed vulnerability assessment of each single building is a very expensive and time consuming process hence department can initially select the building for PVA especially from the seven highly vulnerable districts of the state subsequently from the other districts. This PVA scoring will be supportive in making a decision that whether further stage of vulnerability assessment and retrofitting is required or not in the particular.

When strong earthquake shaking occurs, a building is thrown mostly from side to side, and also up and down. That is, while the ground is violently moving from side to side, taking the building foundation with it, the building structure tends to stay at rest, similar to a passenger standing on a bus that accelerates quickly. Once the building starts moving, it tends to continue in the same direction, but the ground moves back in the opposite direction. Thus the building gets thrown back and forth by the motion of the ground, with some parts of the building lagging behind the foundation movement, and then moving in the opposite direction.

Damage can be due either to structural members (beams and columns) being overloaded or differential movements between different parts of the structure. If the structure is sufficiently strong to resist these forces or differential movements, little damage will result. If the structure cannot resist these forces or differential movements, structural members will be damaged, and collapse may occur.

Building damage is related to the characteristics of the building, and the duration and severity of the ground shaking. Larger earthquakes tend to shake longer and harder and therefore cause more damage to structures. Earthquakes with Richter magnitudes less than 5 rarely cause significant damage to buildings, since acceleration levels (except when the site is on the fault) are relatively small and the durations of shaking for these earthquakes are relatively short. In addition to damage caused by ground shaking, damage can be caused by buildings pounding against one another, ground failure that causes the degradation of the building foundation, landslides, fires & floods etc.

Interior Element Mitigation Measures:

- **Heavy Architectural Exterior Elements**

- o Mitigate Danger Of Falling Heavy Exterior Facade Elements: Cornices, corbels, and other architectural elements are common among historic, unreinforced masonry structures. Such elements are generally constructed of stone or other heavy, brittle materials and often fail due to poor anchorage or bracing. Stone awnings and decorative features may not have proper anchorage or reinforcement. The dead weight added by these elements can increase lateral forces. To reduce damage, heavy non-structural elements should be minimized. Such elements may be removed, relocated, or replaced using lighter materials, or replaced with an independent structure.

- **Windows**

- o Protect Windows That Are Vulnerable To Breakage: Glass windows typically crack or shatter when the frames are distorted or damaged. The principle causes of glass breakage are window frame distortion and inadequate edge clearance around the glass. Stiffening bracing or redesigning of the window frame can reduce future damage. Bracing usually consists of steel tie rods anchored to the corners of the window frame and connected by a turnbuckle. Another method is to use specially designed windows that use wider frames and include a compressible material between the frame and the window glass to avoid direct contact between the window and the frame.

- **Parapets**

- o Provide Tie Backs For Parapets And Heavy Exterior Architectural Elements: Brick parapets are typically mounted along the tops of unreinforced masonry buildings. Parapets are heavy, brittle, and typically collapse near the centers of long walls or at corners. Parapet damage or failure is a common result of earthquakes. Parapets can be braced from the rear using steel angle braces anchored into the parapet and connected to the roof framing. Parapets can also be braced using reinforced concrete or shotcrete placed behind the parapet and anchored. Reducing the height of parapets also reduces the seismic load on the parapet by reducing the weight.

- **Chimneys**

- o Brace or Support Chimneys: Brick chimneys are heavy, brittle, and can fail unless reinforced near the top and supported by the building roof and walls. Chimneys on older buildings frequently suffer damage or collapse during earthquakes. Several retrofit methods can be used to mitigate damage:

- Chimney extensions above the roofline can be secured with steel straps anchored to the roof framing with steel angle braces.
- The chimney flue enclosure can be reinforced using vertical and horizontal bars encased in concrete.
- For multi-storied buildings, chimneys can be anchored at each floor level using steel wrap ties that are anchored to the floor joists.

• Interior Partitions

o Ensure Stability Of Interior Partitions: Interior partitions of all types and ages of buildings are often made of materials that fail when not secured to the floor or roof system. Partitions in older buildings may be constructed of heavy, brittle materials and can topple unless they are braced against the floor or roof of the building.

Interior partitions can fail during an earthquake. Retrofitting can be done with connections that restrict the partitions from sideways movement while allowing vertical movement. Interior partitions generally need lateral support from ceilings or from the floor or roof framing. Unreinforced masonry partitions can also be replaced with drywall partitions.

Unbraced partitions that do not extend to the floor or roof framing should be braced to the framing. Steel channels are sometimes provided at the top of the partition to provide lateral support, and allow some floor or ceiling movement without imposing any loads on the partition.

• Ceilings And Lights

o Ensure Collapse Prevention of Suspended Ceilings And Lights: Suspended ceilings and overhead lighting fixtures typically fail where anchorage is poor, or the runners that support the panels and lights are too weak to withstand lateral earthquake forces. Unbraced suspended ceilings can swing independently of the supporting floor and be damaged or fall. Installing 'four-way' diagonal wire bracing and compression struts between the ceiling grid and the supporting floor will significantly improve the ceiling's seismic performance. In addition to the struts, the connections between the main runners and cross runners should be capable of transferring tension loads.

• Raised Computer Floors

o Ensure Stability of Raised False Floors: Raised floors that support computer equipment are found in many buildings. These floors and the equipment they support can be damaged or destroyed due to inadequate anchorage to the structural floor. Raised computer floors may collapse from earthquake forces. To reduce the risk for this type of damage, anchor the pedestals that support the raised flooring to the building's floor and secure the pedestals to the wall.

Chapter-4: Disaster Preparedness

4.1 Strategies for Disaster Preparedness

For better supervision, monitoring and preventive measures capacity building programme will be launched for officials working at various levels as per their requirements. Capacity building programmes are categorized into two types. One will be for the Senior Officials of the department and the other for Lab Assistants/support staff/Technical Staff. For Senior Officers of the FSL one day advocacy programme will be organised at State level and for others two/three day sensitization programme will be conducted. The team members of FSL will be trained to make their laboratories safe by preparing safety plans and practicing mock drills. Managers of FSL will facilitate the efforts of risk reduction. Trainings for Capacity building will be conducted at two levels:

State Level Advocacy Programme: This programme will be for senior functionaries of the department. It will be of one day duration. Director, Joint Director, Assistant Director, and Deputy Directors of Higher FSL will participate in it from all the offices of the FSL. State Nodal Officer will organize one day advocacy programme. Director/Joint Director will Chair the advocacy programme. This programme can be conducted in coordination with the Department of Health & Family Welfare and Police Department or other stakeholders of the department to mainstream the efforts in the major stakeholder departments.

4.2 Measures for Disaster Preparedness

In case of any disaster, logistics play a vital role in delivery of services. The provision of following items is prerequisite for safety measures in institutions.

1. Necessary Items: Items in this head include power backups, Stretcher, ropes, torch, alternative communication system, Siren, Public addressable system and tents etc.
2. Fixing Non-Structural Elements: It includes fixing of Almirah and other falling hazards that can harm during earthquake.
3. IEC material: Pamphlet, brochures or booklets that can be developed to distribute in the Catchment area of the institutions.
4. Repair of computer, printer, phone, fax etc: Most of laboratories have phones, computers, printers etc. These accessories may be used for warning and information during the period of emergencies. Such equipment need to remain functional.

5. Contingency: It will be used to establish warning and information cell in each building. This cell should be able to communicate with District Emergency Operation Centre. The contingency fund can also be utilised for the requirements of various teams constituted.

Some of the key Pre Disaster Activities to be carried out by Department:

- Formation of Disaster Management Cell and manning the same by senior personnel drawn from key Directorates.
- Incorporating costs for preventive and mitigation measures for earthquake, flood, fire and storm prone areas to construct disaster resistant buildings.
- In association with Fire Dept. getting fire extinguishers installed in laboratories identified and trained in operating them.
- Awareness Generation Programmes about Hazard, the kind of preparedness required and how to act at the time of disaster shall be organized in laboratory on monthly basis.
- Making adequate arrangements for alternate laboratories/mobile laboratories, adequate functional power backup systems in the existing laboratories.

Efforts & Recommendations:

Dealing fire breakout:

- Fire fighting equipment: Fire fighting equipment like fire extinguishers and sand buckets have been installed at various areas that may be susceptible to fire breakout.
- Installation of fire alarms: Fire alarms need to be installed at various zones of the lab that may be susceptible to fire.
- Fire proof vaults and cabinets for storage of case property: Fire proof vaults need to be created in addition to fire proof cabinets for storage of case property and important documents.
- Exit routes in case of Fire: Exit routes in case of a fire breakout have been identified and demarcated.

Dealing earth quakes:

- Exit routes: Exit routes in case of an earth Quake have been identified for each block and their respective floors. All the staff personnel have been made aware of the emergency exit route in case of an earth quake.
- Creation of earthquake proof vaults for storing valuable equipment with HPSEDC.
- Further, keeping in view the diverse nature of the exhibits, the vaults need to design as per the requirement of each division.

Exiting the building in case of an eventuality:-

- **Alarms for Emergency Exit:-**

- Alarms need to install at various location for alerting personnel for an emergency exit.
- The control of the alarms shall be with the security department further alarms should be easily accessible to any individual who is first to sense an emergency.

- **Gathering after Exit and further action:**

- All the personnel have been directed to assemble in parking ground by following the exit routes.
- Once all the personnel have assembled, any one missing shall be identified and efforts to trace the whereabouts of the missing shall be initiated.
- Simultaneously the disaster management authorities, ambulance, local police, fire brigade and home guards shall be intimated about the eventuality.
- Machinery available at the premises shall be pressed into action deal the eventuality till the arrival of specialised man power and machinery.
- First aid kits have been provided at various regions in the building and the same can be put to use.

Chapter-5: Disaster Response and Recovery

5.1 Disaster Recovery Plan & Business Continuity

Business Continuity (BC) and Disaster Recovery (DR) are the watchwords of businesses in the Information Technology (IT) world. The predominant role of Wide Area Networks (WANs) in almost all major fields of business has made it an imperative for IT and Network managers across the globe to accelerate their network infrastructure, and also devise workable BC/DR plans. HPSEDC shall form/strengthen a Disaster Management Cell which will prepare the Disaster Recovery Plans for the departments of the state in coordination with HPSDMA.

The primary objective of a Disaster Recovery plan (or Business Continuity plan) is the description of how an organization has to deal with potential natural or human-induced disasters. The disaster recovery plan steps that every enterprise incorporates as part of business management includes the guidelines and procedures to be undertaken to effectively respond to and recover from disaster recovery scenarios, which adversely impacts information systems and business operations. Plan steps that are well-constructed and implemented will enable organizations to minimize the effects of the disaster and resume mission-critical functions quickly.

Business Continuity or DRP steps involve an extensive analysis of an organization's business processes, IT infrastructure, data backup, resources, continuity requirements and disaster prevention methods.

Secondly, it is the process of creating a comprehensive document encompassing details that will aid businesses in recovering from catastrophic events. Developing a disaster recovery plan differs between enterprises based on business type, processes, the security levels needed, and the organization size. There are various stages involved in developing an effective Disaster Recovery or Business Continuity planning. The key phases and the plan steps are outlined below:

Phase I – Data Collection

1. Project should be organized with timeline, resources, and expected output
2. Business impact analysis should be conducted at regular intervals
3. Risk assessment should be conducted regularly
4. Onsite and Offsite Backup and Recovery procedures should be reviewed
5. Alternate site location must be selected and ready for use

Phase II – Plan Development and Testing

1. Development of Disaster Recovery Plan
2. Testing the plan

Phase III – Monitoring and Maintenance

1. Maintenance of the Plan through updates and review
2. Periodic inspection of DRP
3. Documentation of changes

5.2 Disaster Recovery Plan Criteria

A documentation of the procedures as to declaring emergency, evacuation of site pertaining to nature of disaster, active backup, notification of the related officials/DR team/staff, notification of procedures to be followed when disaster breaks out, alternate location specifications, should all be maintained. It is beneficial to be prepared in advance with sample DRPs and disaster recovery examples so that every individual in an organization are better educated on the basics. A workable business continuity planning template or scenario plans are available with most IT-based organizations to train employees with the procedures to be carried out in the event of a catastrophe.

5.3 DR Team – Roles and Responsibilities

Documentation should include identification and contact details of key personnel in the disaster recovery team, their roles and responsibilities in the team.

5.4 Contingency Procedures

The routine to be established when operating in contingency mode should be determined and documented. It should include inventory of systems and equipment in the location; descriptions of process, equipment, software; minimum requirements of processing; location of vital records with categories; descriptions of data and communication networks, and customer/vendor details. A resource planning should be developed for operating in emergency mode. The essential procedures to restore normalcy and business continuity must be listed out, including the plan steps for recovering lost data and to restore normal operating mode.

5.5 Testing and Maintenance

The dates of testing, disaster recovery scenario, and plans for each scenario should be documented. Maintenance involves record of scheduled review on a daily, weekly, monthly, quarterly, yearly basis; reviews of plans, teams, activities, tasks accomplished and complete documentation review and update.

The disaster recovery plan developed thereby should be tested for efficiency. To aid in that function a test strategy and corresponding test plan should be developed and administered. The results obtained should be recorded, analyzed, and modified as required. Organizations realize the importance of business continuity plans that keep their business operations continuing without any hindrance. Disaster recovery planning is a crucial component of today's network-based organizations that determine productivity, and business continuity.

5.6 Roles and responsibilities of the nodal officers:

Roles and responsibilities of the nodal officer are as under:-

1. Act as the focal point for disaster management activities of the department. The department may ensure that he/she has the mandate to work immediately without waiting for directions from the higher authorities. This will save time.
2. Provide his/ her contact and alternate contact details to SDMA/DDMA and Revenue Department, State and District Emergency Operation Centre, all line departments and agencies.
3. Accountable to any communication/actions related to disaster management of the department.
4. Take lead to prepare the department disaster management plan, Emergency Support Function (ESF) plan and Standard Operating Procedure (SOP).
5. Constitute the Incident Response Team (IRT) in the department as per the need and organize training for members.
6. Help the department to procure the equipment necessary for search and rescue, first aid kits and disburse the same to IRTs and for the department if required.
7. Provide regular information on disaster or task assigned to him to SEOC/ Revenue Department during and after disasters in consultation with the department head.
8. Attend Disaster management meeting, trainings, workshops or any related programme on behalf of the department.
9. Identify an alternate nodal officer and build his/her capacity.
10. As per the need of the department, set up control room and assign other official (s) for

control room duty.

11. Identification and staffs for deployment on site operation centers (on site control room during a disaster)

12. In consultation with the department, make arrangement of alternative communication system for the department.

13. Mobilise resources for disaster response activities as per the resource inventory put in the department DM Plan if it is needed by the department or other line departments.

14. Organise regular awareness programmes in the department.

15. Organise the periodic mock drills at least twice a year as per the suitability of the department and update the plans at all levels and ensure participation of the department in mock drills of other agencies and other departments.

16. To have liaison with other departments and functionaries working in the field of DM.

Chapter 6: Financial Resources for Implementation of DMP

Section 40(2) of the Disaster Management Act stipulates that every department of the State, while preparing the DM Plan, shall make provisions for financing the activities proposed therein. Normally the funds required for risk assessment and disaster preparedness must be provided in the budgets of every concerned Board. Such funds are not very sizeable and HPPCB will allocate such funds within their normal budgetary allocations from coming budget year for risk assessment and preparedness.

HPSEDC should make financial allocations in preparing and executing the disaster management plan. The Director (Finance) should plan for the following:

- Funds for Prevention and Mitigation Activities
- Funds for Preparedness and Training Activities
- Funds for Response Activities (including pre-authorization to draw money from treasury in the event of an immediate emergency)
- Funds for Disaster Risk Insurance
- Funds to strengthen and trainings of Disaster Recovery Planning cell/DM cell

