CRISIS MANAGEMENT PLAN

(CMP-2015)

FOR

TELECOMMUNICATIONS

GOVERNMENT OF INDIA

MINISTRY OF COMMUNICATION & IT

DEPARTMENT OF TELECOMMUNICATIONS

INTRODUCTION

Disaster Management Act, 2005 defines : "Disaster" means a catastrophe, mishap, calamity or grave occurrence in any area, arising from natural or man made causes, or by accident or negligence which results in substantial loss of life or human suffering or damage to, and destruction of, property, or damage to, or degradation of, environment, and is of such a nature or magnitude as to be beyond the coping capacity of the community of the affected area.

A '**natural disaster'** is one that emerges in the environmental settings – be natural, managed or civilized. In understanding the origin of a 'natural disaster' the term 'natural' implies to 'nature' of an event, process, condition or material (a hazard) that is responsible for causing catastrophe, damage or major loss. It may be related to one or more of geological, hydro-meteorological, industrial, urban or other natural environments.

A **'manmade'** disaster is the direct creation/activity of human-being(s) with direct/indirect knowledge of the risk/resultant catastrophe/damage/loss or due to serious human/technical failure and 'hazard(s)' are created or utilized to generate the outcome. These are mostly related to disciplinary performance or security failure, defense/war and mass management/ law & order aspects.

DISASTER THREATS TO TELECOMS SECTOR

Disasters Threats will continually affect the Telecoms Sector and may manifest in isolation or in combination. The increased and complex threat environment of the India, the Telecoms Sector will need to be prepared to mitigate a broader range of threats, often in combination, and necessitating a more coordinated response. The following threat events are being faced by the Telecoms Sector:

- **Loss of Power** – Electricity is the critical component in the running of any telecommunications system. Without a supply of electricity, the system fails. Electricity supply could be caused to fail for a number of reasons, including; over demand, power cable failure, generator failure, deliberate attack or sabotage.
- **Loss of availability of fuel oil** – Fuel oil is used in the power generation through diesel generators for maintenance of telecom systems and it therefore a lack of supply has the potential to disrupt systems. Additionally, maintenance engineers and technicians rely on vehicles to reach parts of the network which require attention.
- **Disruption to land, sea or air transport** – Critical parts of the network may not be accessible for maintenance or upgrade if transportation is denied (through non-availability of fuel, or denial of key routes through natural disaster or conflict zones).
- **Infrastructure failure** – deliberate or unintentional damage to critical components of the physical network such as a break in a subsurface/sub sea fiber optic cable at a single point of failure/point of presence. The loss of multiple, critical network elements within a facility or the facility itself such as a major, network exchange. The loss of this type will have major, network-wide impact affecting end users of multiple services.

- **Telecom System failure** – multiple failure of network elements causing major, service disruption and outages.
- **Software failure** – failure of network wide distributed operating system or control programme software. Software on the live network may not be rolled back without causing network outages.
- **Electronic interference** – degradation or disruption caused by an external source entering the system via the network either intentionally or unintentionally.
- **Large scale temporary absence of staff** – Issues such as pandemic flu or large scale natural disaster could indirectly cause the networks to fail through lack of staff availability for maintenance or manual operation.
- **Permanent or long-term absence of staff -** Certain workers within the sector will be of greater criticality (for example, technical or maintenance engineers). Without these key positions being fulfilled there is again the potential for the networks to fail.
- **Denial of site/geographical area, permanently or for a significant period** – In the event that a specific building, facility, site or region were to be denied (either through damage or destruction – by sabotage, terrorism, or natural disaster – or through loss of access – by contamination or human interference), critical network maintenance or operation could be affected.
- **Cyber Threats -** the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet
- **Embargo** – the prohibition of commerce and trade with a certain country that manufactures equipments used in telecommunication networks within the India.

Telecommunications services play a primordial role in the preparedness and the management of national disasters/emergencies, they provide a platform of communications for the public and the authorities in charge of crisis management to be used in the rescue and relief operations. As natural and man-made disasters often occur without prior warning, preparedness as well as effective and timely response of all possible communication means during those emergencies are crucial to ensure the safety of the public.

The Emergency Telecommunication Plan lays down the sequence of actions to be taken by all relevant agencies in crisis/emergency/disaster situations.

The plan has two parts: - I deals with aspects which are common to all contingencies/emergencies while Part II comprises of Standard Operating Procedures.

Each Telecom Service Provider will prepare Emergency Telecommunication Plan and Standard Operating Procedure to deal any crisis/emergency/disaster related situation.

PRIORITY SERVICES

The Country's telecoms priorities in an emergency are geared towards the provision of telecoms services to priority user groups, and those commercial entities that have contracts in place with the TSPs to ensure a minimum level of service is maintained.

TSPs are required to protect Priority Telecoms Services for the Priority User Groups. Different priority user groups have different requirements for priority telecoms services (for example, individual government VIPs require mobile services as a priority, whereas financial centres require Internet services as a priority). For this reason, the plan does not impose specific technical requirements, which are the responsibility of the TSPs to propose, but the Licensees are required to fulfil the following obligations:

The TSPs shall inform the NTDCC of its plans for implementing any special emergency technical measures and their expected impact on priority users and non-priority users, any gaps shall be identified and remedies to be conveyed to NTDCC. NTDCC may seek NETMC's support to cover the gaps.

Priority Telecoms Services are those services provided by the Telecoms Service Providers which are critical to user operation in an emergency (with specific emphasis on the Priority User Groups).

The normal list of priority services, is based and dependent on the user priority groups and the event

- Voice (mobile* and fixed) services;
  - Fixed-line private circuits and dedicated lines,
  - Mobile phone access overload class/control,
  - Mobile phone precedence and pre-emption,
- Internet services;
  - Internet high bandwidth load shedding to mitigate congestion due to network traffic overloading.
- Data services (leased lines) and data centres; and

Specific priority users will have some or all of these priority services

Priority User Groups

Priority users are those organisations which have operational functions critical to public safety and security during an emergency. The relevant competent authority will specify which entities are priority user groups in the event of an emergency.

The following list summarises the main priority user groups:

- Government agencies
- Health Agencies
- Defence
- Petroleum Production
- Safety and Security Agencies
- Financial Institutions
- Semi government agencies
- Public Emergency Agencies
- Armed Forces
- Utilities

- Red Cross
- NGOs
- Foreign diplomatic missions.

INSTITUTIONAL FRAMEWORK

In disasters/crisis/emergencies, the primary responsibility for organizing response and relief as well as recovery in disaster affected areas lies with the state government. However, where issues pertaining to India's relation with foreign powers or defence, territorial integrity of the country or matters pertaining to national interest or central Government installations are concerned, the State Government will work under policy guidelines laid down by the Central Government while dealing with emergencies.

The Ministry of Home Affairs is the nodal agency at the National level for coordination of response and relief in the wake of natural/manmade disasters (except some ones). The Department of Telecommunications will render Emergency Support Functions (ESF) wherever Central intervention and support are needed by the Central/State Governments.

Real time communication is the backbone of all operations in emergency management whether at the prevention, preparedness or response phases. Although telecommunications are organizational tools for the different phases of disaster management, they also need their own organization and readiness.

This framework consists of an Emergency Telecommunication Plan and following committees for management of telecommunications means prior to, during and post national emergency situations :

i. National Emergency Telecom Management Committee (NETMC) headed by the Secretary (T) at DOT HQ
ii. National Telecom Disaster Coordination Committee (NTDCC) headed by Member (T) at Central Level
iii. State Telecom Disaster Coordination Committee (STDCC) headed by DDG (TERM) at State level
iv. District Telecom Disaster Coordination Committee (DTDCC) headed by DDG (TERM) at District Level

All Telecom Service Providers at the National, State and District Levels will function in accordance with the guidelines and directions given by these committees.

National Emergency Telecommunication Committee

The National Emergency Telecom Management Committee would be the apex body of high-level officials of the Department of Telecommunications for dealing with major crisis/emergency/disaster, which has serious or national ramifications. The composition of the Committee is as under :

i.	Secretary (T)	- Chairperson
ii.	Member (S)	- Member
iii.	Member (T)	- Member
iv.	Member (F)	- Member
v.	Add. Secretary(T)	- Member
vi.	Advisor (O)	- Member
vii.	Advisor (T)	- Member
viii.	Advisor (WPC)	- Member

DDG dealing disaster management will be the Convener of the NETMC. The NETMC will be free to co-opt members depending upon the emergency, as and when required. Disaster Management Cell will keep a copy of updated list of the names of members of NETMC, nodal officers of **all concerned Ministries/Departments/TSPs/Agencies** their telephone/mobile numbers and addresses.

The compositions of the Co-ordination Committees at National, State and District levels are incorporated in SOP.

ROLE OF STAKEHOLDERS

Role of the Telecom Disaster Co-ordination Committee

The Committee will aim at drafting an Emergency Telecommunications Plan (ETP) that would address the procedural and technical issues of managing communications under emergencies. It should ensure the development of all needed regulations and documents of the ETP and its implementation by all stakeholders. Along and prior to the drafting of the ETP, the Committee should fulfil the following responsibilities:

- Ensure that TSPs (private and public) invest in preventive measures that will ensure maximum robustness and preparedness of the telecom networks during emergencies.
- Ensure that TSPs (private and public) develop detailed emergency plans for management of resources under their responsibility.
- Conduct annual reviews of the ETP/SOP
- Organize annual symposium on telecommunications availability during emergency.
- Coordinate with international organizations and experts.
- Update the communications plan according to development and innovations in emergency telecommunications systems.
- Disseminate information among the Public and the Governmental Authorities on the availability of telecom services and equipments for use during emergencies.

- Organize and conduct awareness campaigns on the use of communications systems during disasters.

- Ensure the restoration of the telecommunications network to their normal operations after the end of the emergency situation.

- Follow up ITU-R activities and try to benefit from the ITU's assistance

- Develop technical rules to promote reliable, interoperable public safety radio communications.

- Make use of the ITU starring effort in disaster management, especially the Tampere convention which facilitates the rapid deployment and effective use of telecommunications resources during emergencies.

- Review the international agreements with the neighboring countries for coordination of information, equipment and expertise for disaster management and mitigation.

- Decrease custom duties and restrictions in order to allow humanitarian assistance and equipment from other countries during times of disasters.

- Encourage sharing of infrastructure among relief officers from different government administrations and agencies

Role of the Telecom Service Providers (TSPs)

Public and Private TSPs are the providers of telecommunications services during normal or emergency situations. Therefore it lays upon the responsibility of those public or private operators to develop in accordance with the guidelines of the NTDCC, a plan of action for managing emergency situations. Therefore TSPs should undertake the following actions:

- Assess the different disaster scenarios and match the communications needs with the available resources.

- Assess the needs and capabilities of the response personnel, relief officers, NGOs and other critical users of communications means during national emergencies.

- Develop a well documented emergency action plan for all business. This action plan should be reviewed by the NTDCC

- Develop preventive measures to protect essential infrastructure.

- Perform periodic, well documented and effective tests on the procedures and equipments used during emergencies.

- Develop a clear management structure of the emergency action plan.

- Assign a representative from each operator before the NTDCC, expected to be responsible for, or involved in, the management of the operator's emergency and business continuity.

- Ensure the implementation of the failure notification procedures as detailed in the quality of service regulation issued by the TRAI.

- Sign Memoranda of Understanding between each other (under the supervision of the NTDCC) for the mutual coordination during emergencies.

INFORMATION REPORTING

In case of emergency/disaster, the information flow chart has been incorporated in the Standard Operating Procedure documents.

EMERGENCY TELECOMMUNICATIONS PLAN (ETP)

The Emergency Telecommunications Plan (ETP) is a strategic plan with the corresponding set of rules and regulations that establishes a national and overarching vision for the utilization of telecommunications systems for emergency purposes and guide stakeholders on their specific roles and responsibilities. There are three main axes of the ETP:

a) Readiness of telecommunications systems for emergencies.
b) Emergency Communications Services.
c) Recovery of Emergency Communications Systems.

All these three axes have been incorporated in SOP.

EMERGENCY TELECOMS DEPLOYMENT

Deployable telecoms assets, operated by the Telecom Service Providers, are required to meet the following contingencies:

- **To replace damaged or destroyed telecoms physical infrastructure (e.g. a telephone exchange).**
- **To mobilise deployable mobile phone systems or portable base stations to be in position and operational anywhere on the main cities' roads in the affected area within 8 hrs from being requested. Additional 2-4 hrs are granted for rural areas due to the nature of difficult approach and far distance.**
- **To mobilize deployable Satellite terminals and satellite phones in inaccessible and remote areas.**
- **To provide new facilities to manage the consequences of an emergency (e.g. provide telecom facilities while setting up a large refugee camp in a 'communications-free' area).**
- **Provide a resource availability information to the NTDCC/STDCC and be prepared to rapidly deploy telecommunications assets in accordance with priorities. TSPs are to have fully developed capabilities and solutions within 12 months of issue of the ETP and SOP.**

MEDIA HANDLING

A well thought out media handling strategy and the provision of appropriate, and accurate information to the public is an essential part of ensuring an effective response.

A telecommunications failure represents an additional challenge during the immediate information vacuum in that it should be assumed that day to day means of communication with the national broadcast media will be affected.

Information media representatives will require includes:

- **Update –** general statement on situation, including if appropriate geographical extent and any Casualties
- **Practical Information –** outline public safety advice and support available
- **Action –** outline of actions being taken, status of investigation if appropriate, resources, evacuation
- **Timescales** –outline steps towards restoring the networks and effected Services

POST-EMERGENCY

The phase immediately following the emergency is easily neglected. However, conducting an effective review of the performance of the main actors is essential in ensuring that the key learning points are captured and acted upon in a timely fashion.

TSPs activity

Telecom Service Providers are to:

- Review their performance before, during and after the emergency;
- Update their plans and procedures, should any gaps have been identified.
- Submit a report within two weeks of the declaration of 'emergency over' to the NTDCC outlining the lessons learned and any planned remedial actions.

STDCC/DTDCC activity

Within a month after any emergency there must be a full debrief of the NTDCC and any other STDCC/DTDCC employees who were involved in the response. This will enable the NTDCC to capture as much information about the emergency as possible to improve the NTDCC emergency management procedures. If the NETMC has had any involvement in the emergency then they should also be invited to take part in the debrief.

The debrief must include the following procedures:

- Secure all team records and the log book;
- Compile a report which lists the lessons learned by the STDCC/DTDCC and TSPs – a copy of the report should be provided to the NETMC;
- Assess how the STDCC/DTDCC would have responded if the emergency had escalated further;
- Decide on changes and/or improvements to the emergency management procedures;
- Update the ETP/SOP accordingly;
- Ensure that MoU and directives are appropriate should another emergency occur;
- Communicate to all relevant stakeholders any changes to the way the Telecoms Sector intends to prevent a reoccurrence; and

- Provide any specific continuation training identified as necessary.

Following the receipt of the after action reports from the licensees the NTDCC will compile a consolidated report for the Sector and present it to the NETMC and any other competent authority (once needed) within four weeks of the declaration of emergency over.

ETP MAINTENANCE

Testing and exercising

With rapid advancements in the telecoms technology and the likely continued growth and complexity of the market, it is essential that the Telecoms Sector maintains a high level of preparedness. This will better enable the TSPs to detect potential evolving threats and develop appropriate plans and procedures to respond when issues occur.

The ETP therefore will be subject to a major exercise every two years with desktop exercises every year. The effectiveness of the ETP will be tested against a credible emergency scenario. Where appropriate this exercise will be carried out in conjunction with exercises being undertaken by the NTDCC.

An annual exercise is the minimum requirement, but more regular desktop exercises may initially be required to develop understanding by responders or to address specific issues.

Administration

The ETP will be published by the Disaster management Cell (DMC) of DOT and an electronic version will be held on the official DOT website. The DMC will provide all TSPs with a copy (hard and soft) of the plan.

The DMC will be responsible for agreeing/arranging any amendments to the plan and for ensuring that all copies of the plan are updated promptly in the event of any amendment. The NTDCC is responsible for managing version control of the ETP.

****