NIGERIAN COMMUNICATIONS ACT, 2003

GUIDELINES ON DISASTER RECOVERY, 2023

TABLE OF CONTENTS

NIGERIAN COMMUNICATIONS ACT, 2003

GUIDELINES ON DISASTER RECOVERY FOR THE NIGERIAN COMMUNICATIONS INDUSTRY, 2023

In exercise of the powers conferred upon it by Sections 70, 148 and 149 of the Nigerian Communications Act, 2003 and all other powers enabling it in that behalf, the Nigerian Communications Commission hereby makes the following Guidelines:-

PART I
GENERAL PROVISIONS

1. **Application**

   These Guidelines shall apply to all communications Network facilities and service providers in Nigeria.

2. **Objectives**

   These Guidelines seek to address the major causes of communications system failures such as emergencies, disasters, terrorist or cyber-attacks, loss of infrastructure and Network congestion; and in this regard:

   (1) To provide for a disaster preparedness and recovery regulatory framework for telecommunications Network facilities and service providers.

   (2) To ensure business continuity and information sharing during and after emergencies or disasters.

   (3) To enhance collaboration amongst Network facilities and service providers to facilitate Network resilience and faster restoration of service.

   (4) To mandate Network facilities and service providers to adopt mutual aid agreement.

   (5) To enhance consumer education to better prepare for emergencies.

   (6) To supplement the general regulatory framework on emergency and disaster recovery in Nigeria.

PART II
GENERAL MANDATES ON DISASTER RECOVERY PLAN

3. (1) Every Network facilities and service provider shall have a disaster recovery plan which shall consist of a strategic plan setting out the vision for utilization of communications systems for emergency purposes and guiding the Network facilities and service provider on

its specific roles and responsibilities. The disaster recovery plan shall be in line with Schedules I & II and Annexure A to these Guidelines and incorporate the following:

(a) Preparedness of communication systems for emergencies;

(b) Emergency communications services setting out the priority users; and

(c) Recovery of emergency communications systems.

(2) Every Network facilities and service provider shall establish a disaster management and recovery unit in its organization.

(3) Every Network facilities and service provider shall within three (3) months from the commencement of these Guidelines submit a disaster recovery plan to the Commission for approval, and the Network facilities and service provider shall designate one of its senior management staff to oversee the disaster recovery plan.

(4) Every Network facilities and service provider shall during emergency situations promptly notify the Commission of any outages in line with its disaster recovery plan as it affects stakeholder notification plan.

(5) Every Network facilities and service provider shall establish, at least, a bi-annual comprehensive test and exercise schedule for its disaster recovery plan to ensure a state of readiness.

(6) Every Network facilities and service provider shall review and conduct a simulation test of its disaster recovery plan every time it makes a critical change to its business environment.

(7) Every Network facilities and service provider shall provide the Commission with its testing and maintenance program in line with the following:

(a) Provide a "Test Calendar" that shows the different test types and their frequency, sequence and dependency on the other tests;

(b) Provide the objectives of each test, list of participants, scope, schedule, prerequisites, outcomes and documented results to facilitate audit by the Commission;

(c) Invite the Commission to attend the testing of its disaster recovery plan, giving a notice of at least one week;

(d) Ensure that the disaster recovery plan is based on the generic 'Table of Contents for a disaster recovery plan' provided in Schedule II;

(e) Undertake a risk analysis and business impact analysis in respect of all their systems at least once every two years or every time it makes a critical change to its business environment;

(f) Apply a staged approach to testing of the disaster recovery plan to minimize the risk to the production environment;

(g) First undertake a 'table-top-exercise' to raise the awareness of the business functions involved and highlight any obvious exposures in the plan; in the second stage, conduct functional testing for various functions. These should highlight problems with the disaster recovery plan which can be modified accordingly; and in the last stage, conduct the "production test", i.e., full-scale testing, where the disaster recovery plans are fully exercised;

(h) Analyse the test results against disaster recovery objectives to identify improvements and modifications to the disaster recovery plan; and

(i) Review the disaster recovery plan within its organization, at least once annually, to identify any revisions to the plan based on the changes that might have occurred in the organization's business, structure, systems or personnel.

(8) In addition to the foregoing provisions of this section, Network facilities and service providers shall submit a report to the Commission of any change in the Disaster Recovery Plan (DRP) for approval.

4. (1) In the event of a disaster, every Network facilities and service provider may deploy its communication assets or collaborate with other Network facilities and service providers to address disaster recovery situations.

(2) The deployable communication assets of Network facilities and service providers shall meet the following contingencies:

(a) To replace damaged or destroyed telecommunications physical infrastructure;

(b) To mobilise deployable mobile phone systems or portable base stations to be in position and operational in strategic areas in the main cities in the affected area within eight hours upon request and not more than twelve (12) hours for rural areas;

(c) To mobilize deployable satellite terminals and satellite phones in inaccessible and remote areas;

(d) To provide new facilities to manage the consequences of an emergency; and

(e) To provide resource availability information to the Committee and be prepared to rapidly deploy communications assets in accordance with priorities defined in these Guidelines.

5. There shall be a Disaster Recovery Coordination Committee for the Nigerian Communications Industry in Nigeria to deal with crisis or disaster, coordinate disaster recovery efforts and prepare and submit a consolidated report for the sector on every disaster for presentation to the Commission comprising;

(a) Designated Management staff of the Commission.

(b) Designated Management staff of the Network facilities and service providers to be approved by the Commission.

6. (1) In addition to such other conditions contained in its operating license, a Network facilities and service provider shall comply with the following:

(a) Provide public emergency call services to first level responders;

(b) Make plans for rapid restoration of services during public emergency situations after necessary consultations with relevant agencies, and implement them; and

(c) Provide priority fault repair services to first level responders.

(2) No Licence to operate any communications system or facilities, or provide a communications service in Nigeria shall be issued or renewed without an approved disaster recovery plan submitted to the Commission from the date of the publication of these Guidelines.

PART III
RESPONSIBILITIES OF THE NETWORK FACILITIES AND SERVICE PROVIDER

7. In addition to such other responsibilities provided in Part II and Schedule I and II to these Guidelines, every Network facilities and service provider shall at all times:

(1) Develop and update its disaster recovery plan, and submit it to the Commission for periodic review and approval.

(2) Develop and implement procedures to improve disaster preparedness and notification.

(3) Assess the needs and capabilities of its response personnel and other critical users of communications services during emergencies.

(4) Develop and submit a comprehensive emergency action plan to the Commission for review by the Disaster Recovery Coordination Committee.

(5) Develop preventive measures to protect essential communications infrastructure.

(6) Develop a user-friendly structure for implementation of the emergency action plan.

(7) Notify the Commission of its representative to the Disaster Recovery Coordination Committee, who shall be a person responsible for or involved in the management of its emergency and business continuity plan.

(8) Implement failure notification procedures as detailed in the Quality of Service parameters issued by the Commission from time to time.

(9) Sign mutual aid Agreement with other Network facilities and service providers for coordination during emergencies.

(10) Develop capacities and design solutions within twelve months of the approval of the disaster recovery plan by the Commission.

(11) Develop and implement procedures for improved disaster preparedness and notification in line with the Schedules to these Guidelines.

(12) Establish disaster recovery teams that can be quickly deployed in the aftermath of a disaster for rapid restoration and repair of any damaged telecommunication facilities in line with Schedule II of these Guidelines.

(13) Design and implement corporate awareness campaigns to ensure successful disaster recovery in the event of an emergency.

(14) Create reliable means of public communication during disasters. To this end, Enhanced Multi-Level Precedence & Pre-emption" (as per 3GPP Technical Standard TS23.067) (eMLPP) based priority call routing scheme should be instituted to ensure that calls of personnel responsible for 'response and recovery' during disasters are routed on priority.

(15) Secure all necessary facilities and installations required for disaster recovery.

(16) Submit an annual report on disaster recovery planning and implementation efforts to the Commission.

(17) Notify the Commission of any outage, crisis or disaster and provide status updates till service is restored.

(18) Disseminate warning messages authorized by the Commission to its subscribers.

(19) Identify procedures to create awareness and educate consumers on the usage of communications services during disasters.

(20) Implement roaming arrangement in line with the framework established by the Commission upon the activation of the Disaster Information Reporting System.

PART IV
RESPONSIBILITIES OF THE REGULATORY AUTHORITY

8. The Commission will:

(1) Take all necessary steps or measures to support other relevant agencies within the national disaster management framework before, during and after disaster situations.

(2) Establish a harmonized narrow band of 5 MHz for all public protection and disaster relief equipment, to allow easy compatibility of equipment of various responder organizations and support First Level Responders to acquire equipment based on the same standard, preferably the standard ETSI TETRA (Terrestrial Trunked Radio).

(3) Mandate every Network facilities and service provider to:

(a) Develop and submit its disaster recovery and business continuity plan; and

(b) Comply with the provisions of paragraph 7(16) of these Guidelines;

(4) Mandate Network facilities and service providers to create awareness regarding the designated emergency number 112 assigned for use by subscribers before, during and after emergency.

(5) Liaise with the Committee to establish a system of receiving disaster warning alert messages.

(6) Further to the provisions of paragraph 3(6) and 7(c) of these Guidelines, attend and monitor the disaster recovery plan tests of any Network facilities and service provider.

(7) Instruct all Network facilities and service providers on information and resources sharing in such circumstances as may be required for public safety.

(8) Allocate the range for emergency communications equipment.

(9) Coordinate with the relevant authorities to receive authorized disaster warning messages and pass these to the Network facilities and service providers for immediate action.

(10) Specify the relevant authorities under the Act that will facilitate the design and development of the disaster recovery plan of Network facilities and service providers'.

(11) Monitor compliance with the provisions of these Guidelines.

PART V- RESPONSIBILTIES OF THE COMMITTEE

9. The Committee shall undertake the following responsibilities:

(a) Coordinate and monitor implementation of mutual aid agreements among the Network facilities and service providers for disaster management;

(b) Identify procedures to create awareness and educate consumers on the usage of communication facilities and services during disaster times;

(c) Establish a system of receiving disaster warning alert messages.

(d) Coordinate with the First Level Responders to facilitate the accomplishment of their disaster recovery activities; and

(e) Recommend to the Commission various measures to facilitate service recovery.

PART VI
MISCELLANEOUS

10. Interpretations

In these Guidelines, unless the context otherwise requires: -

'Act' means the Nigerian Communications Act, 2003;

'Communications system failure' means multiple failures of network elements causing service disruption and outages;

'cyber-attack' means acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the internet; damage to a computer within the definition of the Cybercrime Act, 2015;

'Commission' means the Nigerian Communications Commission;

'Committee' means Disaster Recovery Coordination Committee;

'Denial of Service Attacks (DoS)' means any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.

'Disaster' includes a catastrophe, mishap, calamity, heavy rain, flood, landslides, high tide, fire, terrorist attack or grave occurrence of any kind, 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 causing interruption to business and services or degradation of environment, and is of such a nature or magnitude as to be beyond the coping capacity of the community in the affected area;

'Disaster Information Reporting System' means a system wherein the Commission activates disaster reporting by communicating to the respective Network facilities and service providers on the existence of an emergency and the areas to be covered. The Network facilities and service providers in turn share their Network status information with the Commission quickly and efficiently, who in turn communicate the Network status of the facilities Network and service providers to agencies of government involved in disaster management and recovery.

'Disaster Management Reporting System' means a web-based system that Network facilities and service providers use in reporting communications infrastructure status and situational awareness information during times of disaster or emergency;

'Disaster Preparedness' means putting in place procedures to increase resilience of the Network and other infrastructure to confront any disaster and mitigate its potential impact;

'Disaster Recovery' means putting in place procedures to be undertaken to restore normalcy of operations in the aftermath of disasters, and includes identifying the recovery strategies for all critical business functions, establishing recovery management organization and process, and creating recovery plans for various levels of business functions;

'Disaster Recovery Plan' means a clearly defined and documented plan of action for use at the time of crisis.

'Disaster Recovery Coordination Committee' is a standing committee established by the Commission to coordinate the Disaster Recovery Plans of Network facilities and service providers and to oversee the implementation of these Guidelines on behalf of the Commission;

'Emergency Support Function' means a system that supports restoration of communications infrastructure, co-ordinates communications support to response efforts, facilitates the delivery of information to emergency management decision makers, and assists in the stabilization and re-establishment of systems;

'First Level Responders' are the agencies that are immediately involved in rescue and recovery operations at the disaster site(s) including but not limited to National Emergency Management Agency, States Emergency Management Agencies, Fire Service, Nigeria Police, Federal Road Safety Corps, Nigerian Security and Civil Defence Corp and healthcare providers;

'Guidelines' means the Disaster Recovery Guidelines for the Nigerian Communications Industry;

'Infrastructure failure' means deliberate or unintentional damage to critical components of the physical Network such as a break in a subsurface and sub-sea fibre optic cable at a single point of failure and point of presence and includes the loss of multiple, critical network elements within a facility or the facility itself such as a major network exchange, damage to Network as a result of force majeure;

'ICT' means Information and Communications Technology;

'Network facilities provider' and **'Network service provider'** means Network facilities provider and 'Network service provider as defined under the Nigerian Communications Act, 2003;

'Resilience' means the ability of an organization, staff, system, Network, activity or process to absorb the impact of a business interruption, disruption and loss and ensure continuity of basic services to the end user;

'relevant authority' means any authority for the time being saddled with rescue and recovery responsibility in emergency situations, including but not limited to National Emergency Management Agency, States Emergency Management Agencies, Fire Service, Nigeria Police, Federal Road Safety Corps, Nigerian Security and Civil Defence Corp and healthcare providers;

'Supervising Ministry' means the Ministry for the time being in charge of Communications;

'Tabletop exercise' means a disaster preparedness activity that brings together heads of lines of business and leaders of business processes to evaluate their state of readiness for crisis management, disaster recovery and business continuity through the review and discussion of various time-phased realistic emergency situations or scenario; discuss the actions to be taken in a particular emergency; undertake the testing of emergency plan; clarify roles and responsibilities of heads of line and leaders of business in emergency situation and identify additional mitigation and preparedness needs or action plans for continued improvement of the emergency plan.

11. These Guidelines may be cited as Disaster Recovery Guidelines for the Nigerian Communications Industry, 2023.

Issued this 17th day of February 2023

Professor Umar Garba Danbatta, FNSE, FRAES, FAEng, FNIEEE

Executive Vice Chairman / CEO
Nigerian Communications Commission

SCHEDULE I

Paragraph 3 (1)

DISASTER PREPAREDNESS, RECOVERY AND COMMUNICATIONS GUIDELINES FOR ALL TELECOMMUNICATIONS NETWORK FACILITIES AND SERVICE PROVIDERS

1.0 DISASTER PREPAREDNESS

Every Network facilities and service provider shall ensure the security and resilience of their facilities against potential disasters by implementing the following:

(a) Maintain appropriate protection for telecommunications assets;
(b) Prevent unauthorized physical access, damage to and interference with business premises;
(c) Ensure effective and secure operation of telecommunication facilities; and
(d) Safeguard information in Networks, and secure operation of information processing facilities.
(e) Every Network facilities and service provider shall include a list of the Disaster Preparedness procedures implemented by it in the Appendix of its Disaster Recovery Plan.

1.1. Telecommunication Asset Management

A Network facilities and service provider shall adopt the following:

(a) Identify its telecommunication assets and maintain an inventory;
(b) Designate an individual or entity responsible for telecommunication services maintenance, use of, and access to telecommunication assets;
(c) Classify information and outputs from systems handling confidential data, in terms of their value, sensitivity and criticality to the telecommunications organization; and
(d) Develop appropriate procedures for information labelling and handling, in accordance with the classification scheme adopted by the Network facilities and service provider. Procedures for information labelling need to cover information assets in physical and electronic formats.

1.2. Physical Security

A Network facilities and service provider shall adopt the following:

(a) Use security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) to protect areas which contain switching, transmission, operation and information processing facilities;
(b) Protect secure areas by appropriate entry controls and intrusion detection devices to ensure that only authorized personnel are allowed access;

(c) Design and apply additional physical security for offices, rooms and facilities against damage from fire, flood, earthquake, and other common environmental threats as well as unauthorized access;
(d) Wherever practicable, not concentrate essential equipment, particularly in one building, to the extent that overall Network security is jeopardized;
(e) Utilize underground line plant, buried at a depth where intrusions are unlikely, over an aerial line plant;
(f) Where appropriate, provide diverse cable entry points to sites or buildings and use diverse duct tracks or routes;
(g) Use suitable detection and extinguishing systems for fire; and detection systems for explosive and asphyxiating gases, and floods;
(h) At sites, prone to flooding, utilize the buildings such that the most critical functions are performed in parts of the building with the lowest risk;
(i) Protect equipment from power failures and other disruptions caused by supporting utilities by-

(i) Providing an uninterruptible power supply to all key equipment to ensure service is not disrupted in the event of disruption of main power supply;

(ii) Using duplicate main supplies from separate sub-stations;

(iii) Ensuring supply of fuel for back-up generators with contracts for replenishment;

(iv) Considering alternate sources of power like renewable energy, including on-site wind turbines and solar power to reduce dependency on third party energy suppliers; and

(v) Having enough spares in air conditioning equipment to serve the peak load even if one unit is offline for maintenance and another unit fails.

(j) Protect the power and telecommunications cabling carrying data or supporting information services, from interception or damage by using water-contamination resistant cabling of a level compatible to their flashpoint in accordance with following standards:

(i) For critical fiber optic cables, the standards shall be the UK-MOD Def-Stan 60-Part 3 or the equivalent American standard MIL-PRF8504518A;

(ii) For lower priority cabling the ability to stand water immersion of at least 2 days or compliance with IEC 60974-1-2-FSB standards; and

(iii) For armoured underground telecommunications, EEMU A 133 "Specification for Underground Armoured Cable Protected against Solvent Penetration and Corrosive Attack" or its equivalent standard.

(k) Install systems such as interactive voice response at call centres, to replace manual operations in the event that staff are unavailable during or in the aftermath of a disaster;

(l) Implement a range of controls to achieve and maintain security in Networks, in particular:

(i) Transmission facilities such as transmission cables should be well maintained and, in case of emergency situation, the facilities should be repaired as quickly as possible;

(ii) Single Point of Failure analysis should be conducted and measures put in place to ensure that no single points of failure exist across the Network, as far as is practically possible. Where Single Point of Failure involves third parties who the Network facilities and service provider has no influence or has minimum influence over negotiations should be conducted with the third party to agree on mitigation actions, possibly involving sharing the cost;

(iii) Switching facilities for telecommunication services should be well maintained and their traffic load should be monitored constantly and, in case of an emergency situation, the traffic should be promptly switched to back-up facilities or other routes in order to avoid traffic congestion;

(iv) In the case of denial of service attacks (DoS), switching facilities including routers shall process a higher volume of traffic than in ordinary situation, and the Network facilities and service providers shall implement a control to limit the traffic to an allowable level;

(v) Within the data centre, IT equipment serving business critical systems should, where practicable, be of high availability; and

(vi) Deploy an effective Network management system that covers fault management, configuration management, performance management, security management and traffic management.

1.3 Communications and Operations Management

A Network facilities and service provider shall adopt the following:

(a) Establish incident management responsibilities and procedures (including an escalation process) to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trails and logs;

(b) Implement procedures for faults to be reported and corrective action taken;

(c) Maintain equipment effectively to ensure its continued availability and integrity, in particular:

(i) Make arrangement for the use of suitable alternatives in cases where normal maintenance access to a site may be jeopardized because of bad weather;

(ii) Where third party maintenance contractors are used, the Network facilities and service provider should enter into Service Level Agreements with maintenance suppliers incorporating low response times (less than 4 hours) from the time of notification of equipment failure. The response time should be related to the Recovery Time Objective of systems that are supported by the equipment;

(iii) Make an in-depth spares requirements analysis to determine which spares should be purchased and kept on-site for emergency; and

(iv) Make pre-arrangements with major suppliers to bring in support teams in emergency or disaster situations.

1.4 Information Security

Network facilities and service providers shall develop an information access control policy, define and document the telecommunication business requirements for access control, and restrict access to authorized users only.

1.5 Resilience of Building to Disasters

1.5.1 Network facilities and service providers shall ensure that their buildings are designed to be as resilient as possible to resist or minimise disasters. Network facilities and service providers shall consider the following:

(a) Buildings should not be located in areas with a history of flooding or landslides or close to where significant mineral extraction has taken place or under a flight path to a major civilian or military airport.

(b) Landscaping of the area should be done considering:

(i) High banks or rows of trees (2 meters) be used as mitigation action with respect to vehicle impact and terror attacks;

(ii) Car parks shall be located outside the perimeter fence or, if within, they shall be several hundred metres from the building.

(c) Vehicle security and access control functions complete with barriers shall be located at the perimeter at least 60metres from the building. All mechanical access control functions shall be resilient with 'fool-proof' actions if the access control staff or systems are compromised. They shall however have a manual override to allow access by emergency service vehicles.

1.5.2 A Network facilities and service provider shall adopt effective fire detection, warning and extinguishing procedures and comply with the following:

(a) Rooms in the building should be fitted with smoke detectors with manual pull-alarms both of which shall be tested at least twice annually;

(b) A fire alarm system shall be in place and periodic tests (scheduled and random tests) of the fire alarm system shall be taken; and

(c) An inert gas fire eradication system shall be installed and cover all business critical parts of the building. The gas-based eradication system shall be backed up by a water sprinkler system and hand-held fire extinguishers. Each gas bottle shall incorporate a gauge to show gas pressure with a threshold pressure below which it should be replaced. A maintenance contract should be in place to ensure the replacement of gas within 24 hours of notification.

(d) Each building shall have a central monitoring system monitored by security and accessible to first level responders for all smoke detectors, fire alarms and eradication systems. The central monitoring system shall identify the operating status and "alarm" condition of each smoke detector, alarm and eradication system component.

1.5.3 A Network facilities and service provider shall adopt air handling procedures, in particular:

(a) The air conditioning plant shall be high availability in design, incorporating component level redundancy;

(b) An N+2 philosophy shall be adopted with respect to air conditioners to allow for maintenance of units to take place without any impact on the business even if one air conditioner fails;

(c) All air conditioning equipment shall be connected to the UPS;

(d) Where the air conditioners use a coolant gas such as Freon, consideration should be given to carrying a stock of gas on site;

(e) A regular maintenance schedule shall be in place for air conditioners. For any air conditioners with a 'Mean Time to Repair' greater than Recovery Time Objective of the systems that they support, it is essential that a hot standby air handler be available along with a method to switch between units;

(f) All of the air conditioning units shall be connected to at least two independent mains power supplies;

(g) The air conditioners shall be connected to an environmental monitoring system which can identify any problems with each unit and highlight hotspots in the switch/computer room; and

(h) A comprehensive Maintenance Schedule shall be established to ensure the regular replacement of air-handling filters, maintenance of refrigerant levels, and proper system operations.

1.5.4 A Network facilities and service provider shall have a water detection and protection systems, in particular:

a) No water or waste pipes shall be located above the computer room, or switch room.
b) Water detectors shall be installed in the ceiling space above the business-critical rooms, and in the floor below the rooms.
c) Channelling shall be installed in the floor and ceiling to direct water away from the switch room or computer room.
d) Drains shall be installed to allow any water that enters the room to drain away into a lower level;
e) All water detection and protection systems shall be connected to an environmental monitoring system to identify the individual operating status and "alarm" condition of each of the system components.

1.5.5 A Network facilities and service provider shall provide environmental monitoring systems, in particular:

(a) All security and environmental protection systems shall be monitored by a comprehensive environmental monitoring system, the operations area of which shall be located significantly away from the business-critical room;

(b) There shall be a backup operations area for the monitoring system, located in a different site; and

(c) All security or operations area staff shall be trained to recognize the symptoms of potential disaster and act accordingly.

1.5.6 A Network facilities and service provider shall provide a within-building access control system as follows:

(a) One entry point which is secured via an electronic access control system along with at least two emergency exit points both of which are connected to an audible alarm if opened other than in an evacuation;

(b) A combination of electronic access control and human security interfaced with a thorough initial screening of employees through the Human Resources vetting function;

(c) The electronic access control systems implemented shall be appropriate to the level of sensitivity of the building and data contained therein; and

(d) CCTV cameras shall be installed to ensure safety of staff members and prevent sabotage or theft.

1.5.6 A Network facilities and service provider shall have a plant room to house generators and air conditioning units, which shall have hermetically sealed doors to protect the equipment from the effects of dust storms or flash floods, and ensure that the air intakes of the generators are at least one meter from the ground to eliminate risks from flash floods.

2.0 EMERGENCY COMMUNICATIONS

2.1 Responsibilities of Network facilities and service provider in Emergency Communication

A Network facilities and service provider shall:

(a) Ensure that in applying the priority routing scheme, communications between first responders are routed first;

(b) Give priority for at-risk communities during disasters;

(c) Enter into mutual aid agreement and ensure that the priority call routing scheme is supported through roaming arrangement, such that where the Network of one of the Network facilities and service providers is down or non-functional due to physical infrastructure failure, their subscribers can get access and priority from some other Network facilities and service provider whose Network is up and running; and

(d) Implement awareness programs for spreading awareness about correct usage of telecommunications services by users during disasters, in order to avert the behaviour of users not disconnecting calls for a long time once a call connects.

SCHEDULE II

(Paragraph 3)

STRUCTURE AND CONTENT OF DISASTER RECOVERY PLAN

1.0 The primary aim of disaster recovery planning is to ensure that business processes are restored within the agreed recovery time in the event of an unplanned interruption to service or denial of access to staff.

1.1 A Network facilities and service provider shall ensure that the disaster recovery plan is:

(a) Written and disseminated so that the staff who are familiar with the organization but not the function can implement the plan in a timely manner;

(b) Specific regarding what conditions should trigger its implementation;

(c) Specific regarding what immediate steps are to be taken during a disruption;

(d) Flexible to respond to unanticipated threat scenarios and changing internal conditions;

(e) Focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption;

(f) Specific regarding disaster recovery and continuity teams and contact lists of critical personnel; and

(g) Effective in minimizing service disruptions.

1.2 Every disaster recovery plan shall:

(a) Document strategies and procedures to maintain, resume, and recover critical business functions and processes and should include procedures to execute the plan's priorities for critical and non-critical functions, services and processes;

(b) Describe in some detail the type of events and decision points that would lead up to the formal declaration of a disaster and the process for invoking the plan.

(c) Put in place coordinated responses that reflect the nature of the outage, and should describe the responsibilities and procedures to be followed by each of the disaster recovery continuity teams and critical personnel; and

(d) Describe in detail the procedures to be followed to recover each business function affected by any disruption and should be written in such a way that staff who are familiar with the organization but not the function can implement it in a timely manner.

1.3 Every Network facilities and service provider shall set up crisis management systems and processes and carry out the following steps;

(a) Raise awareness within the organization highlight the responsibilities of both individual and departments;
(b) Audit the organization to identify the level of exposures and mitigating measures that could be put in place;
(c) Undertake a service classification analysis in order to establish, from a business perspective, the business criticality and desired recovery sequence;
(d) Develop appropriate recovery strategies for business, facilities, Network operations and technical functions;
(e) Obtain the resources required to implement the recovery strategy; and
(f) Assist the Disaster Recovery Test Execution Team in testing the plan.

1.4 Every Network facilities and service provider shall design a risk assessment process to identify and analyze the types of risk and their impact on the organization. The assessment should include the following:

a. Types of potential disruptions that could impact the business;
b. Potential business disruptions based upon severity and likelihood of occurrence and how the Network facilities and service provider would respond if:
    i. Critical personnel are not available;
    ii. Critical buildings, facilities, or geographic regions are not accessible;
    iii. Equipment malfunctions (hardware, telecommunications, operational equipment);
    iv. Software and data are not accessible or are corrupted;
    v. Vendor assistance is not available;
    vi. Utilities are not available; or
    vii. Critical documentation and records are not available.

1.5 Every Network facilities and service provider shall have a recovery strategy to restore operations quickly and effectively following a service disruption. The recovery strategy shall:

a. Identify and document alternate recovery strategies for backup, alternate sites and equipment replacement;
b. Identify resources required for resumption and recovery; and
c. Perform a cost-benefit analysis to identify the optimum recovery strategy

1.6 Every Network facilities and service provider shall have the following disaster recovery teams and assigned responsibilities:

(a) Primary Teams which shall be activated where a disaster is declared:

i. **Crisis Management Team:** This is the supreme decision making body with respect to a disaster, although it may delegate executive powers to the Emergency Response team for the initial period (usually 48 hours) of disaster response.

ii. **Emergency Response Team:** This team coordinates response to a disaster (once it has been declared by the Crisis Management Team) for the critical initial 48 hours. This period may be extended at the discretion of the Crisis Management Team.

iii. **Incident Management Team**: This team identifies, reports, analyses, assigns, resolves an incident which may lead in the short or long term to a disruption of normal processing of all or part of the business workload;

iv. **Business and Technical Recovery Team:** This team is responsible for conducting recovery of business operations. Each critical business unit will have a designated recovery team to perform the tasks necessary to recover these business functions.

The team shall also be responsible for restoration of the operational systems and communication functions of the business. In this capacity, the team leader will provide recovery direction and problem resolution, monitor progress, and report recovery status to the leader of the business continuity team. The team may delegate several technical recovery tasks to address areas such as application systems recovery, operational environment recovery and IT recovery;

v. **Business Continuity Team:** The role of the business continuity team is to coordinate the recovery teams' effort and notify the team leader of the crisis management team.

(b) Secondary teams which may be established for specific functions as the nature of the disaster dictates. The secondary team may include the following:

i. **Damage Assessment and Facilities Restoration Team**: This team will assess the extent of damage to the serviceability of premises and infrastructure, secure the protection of all physical infrastructures, co-ordinate with insurance firms and carry out new procurement and replacement if required.

ii. **Communications Team:** The Communications team will be the sole source of communication for the transmission of information to all external and internal parties;

iii. **Administration and Staff Welfare Team**: This team will be responsible for coordinating and easing the logistics in relation to business unit and recovery team staff with regard to combating a disaster.

1.7 Every Network facilities and service provider shall ensure that its disaster recovery plan, also addresses notification to all relevant agencies as specified in Part V of these Guidelines and the following:

a. Clients and other organizations who have contractual arrangements with the Network facilities and service provider;
b. Major shareholders of the Network facilities and service provider;
c. Board members who are not directly involved in the Crisis Management Team; and
d. Representatives of workers' union.
e. Representative of Community

1.8 The information to be communicated by the Network facilities and service provider shall include but not be limited to the following:

a. The locations impacted by the disaster;
b. Services affected by the disaster;
c. Anticipated contraventions of regulations likely to be occasioned by the disaster;
d. Details of any impact on other telecommunications Network facilities and service providers;
e. The assistance to be rendered by other Network facilities and service providers; and
f. Future action plans to prevent similar occurrence.

1.9 The disaster recovery plan shall contain the following:

a. Purpose of the recovery plan;
b. Issues addressed and those not addressed in the plan;
c. Organizations business functions and managerial organogram;
d. Application recovery plan addressing the failure of any specific hardware;
e. Facilities recovery plan addressing the failure of any facilities and infrastructure that supports the Network facilities and service provider's corporate systems. This plan will include evacuation plans for the buildings.

f. Network operation plan addressing failures in the Network itself or the facilities underpinning it such as mobile switching centres or base station controllers.
g. Business unit recovery plan designed to allow each business unit to recover from disasters that may vary in magnitude from the major disasters that impact the whole corporate entity.
h. Location recovery plan designed for critical locations that may have multiple business units. This plan would allow coordination of the restoration of business activities across the various Business Units and facilities at the critical location with minimum confusion, disruption and cost.
i. Organizational recovery plan addressing the unavailability or limited availability of staff or functions as a result of any disaster prevention and mitigation procedures.
j. Work area recovery plan addressing situations where an individual work area may be rendered unavailable.
k. Stakeholder notification plan setting out actions to be taken once a system disruption or emergency has been detected or appears to be imminent;
l. Sequence of recovery activities and the estimated time to restore services;
m. Reconstruction, recovery strategy and procedures setting out the following:

i. Obtaining authorization to access damaged facilities and/or geographical area
ii. Obtaining necessary office supplies and work space
iii. Obtaining and installing necessary hardware components
iv. Obtaining and loading backup media
v. Restoring critical operating system and application software
vi. Restoring system data
vii. Testing system functionality including security controls
viii. Connecting system to Network or other external systems
ix. Operating alternate equipment successfully

n. Any other vital information for effective disaster recovery.

ANNEXURE A

(Paragraph 3)

Disaster Response and Recovery Fail-over Flow Diagram

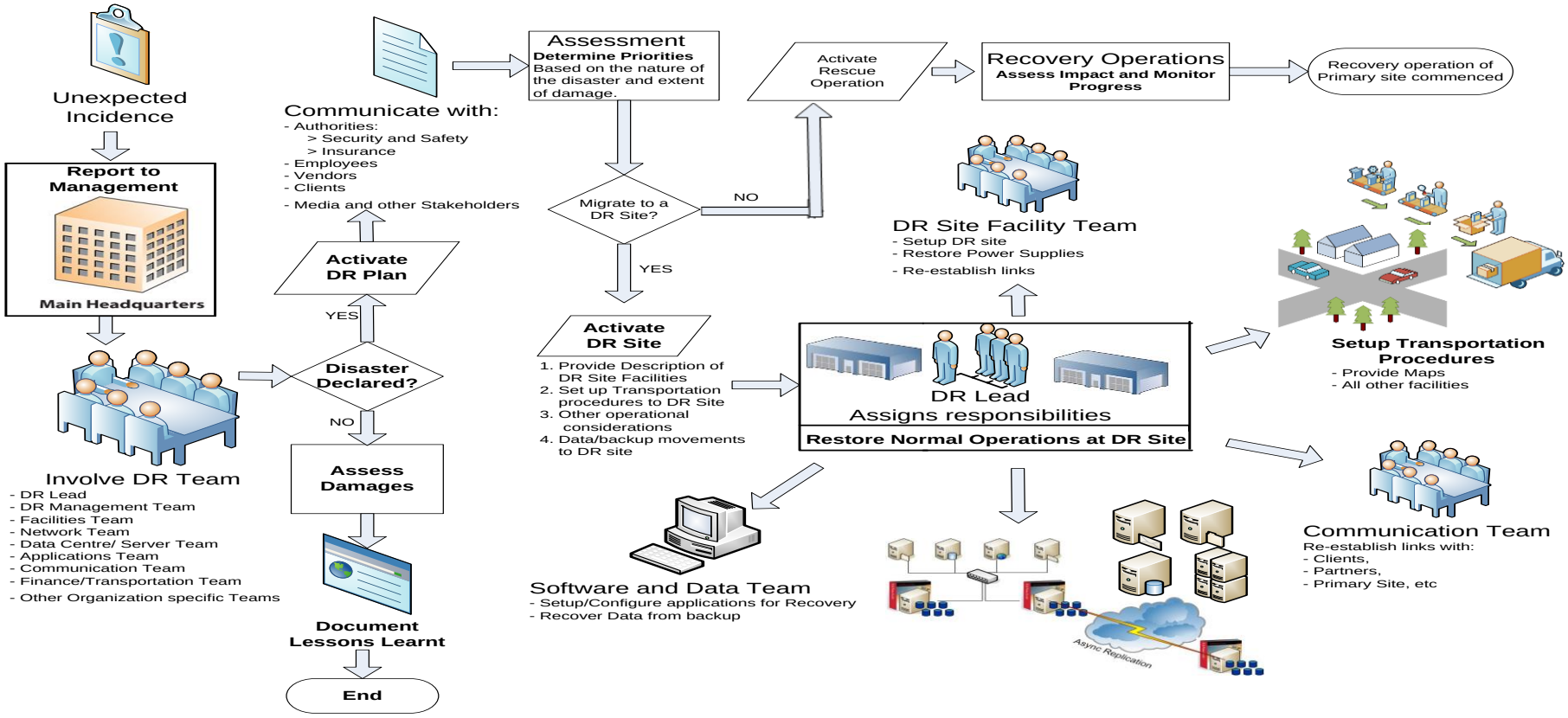

Figure 1: Flow Diagram for Fail-Over Procedure to a Disaster Recovery Site from Main Site