

CHECKLIST OF DISASTER RECOVERY PLAN

S/N	Provisions	Covered	Not Covered	Remarks
1.	Purpose of the recovery plan;			
2.	Issues addressed and those not addressed in the plan			
3.	Organizations business functions and managerial organogram			
4.	Application recovery plan addressing the failure of any specific hardware			
5.	Facilities in the 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			
6.	Network operation plan addressing failures in the Network itself or the facilities underpinning it such as mobile switching centres or base station controllers.			
7.	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			

8.	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.			
9.	Organizational recovery plan addressing the unavailability or limited availability of staff or functions as a result of any disaster prevention and mitigation procedures			
10.	Work area recovery plan addressing situations where an individual work area may be rendered unavailable.			
11.	Stakeholder notification plan setting out actions to be taken once a system disruption or emergency has been detected or appears to be imminent			
12.	Sequence of recovery activities and the estimated time to restore services			
13.	Reconstruction, recovery strategy and procedures setting out the following: i. Obtaining authorization to access damaged			

	<p>facilities and/or geographical area</p> <ul style="list-style-type: none"> 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 			
14.	Any other vital information for effective disaster recovery			