Network and Communication Infrastructure

This section provides guidelines and requirement for deployment of IT networks across institutions in three categories:

- Network Design
- Network Implementation
- Network Management

Network Design

- **Number of users in the institution:** identify the number of network users both onsite and offsite.
- **Services accessed or offered by the institution:** services should be defined and categorized depending on processes and availability requirements
- **Broadband technology:** should be chosen according to location, institutional business requirements, and offices set up. Wireless local area networks are advised for convenient and modernized work spaces
- **Bandwidth requirement1:** minimum bandwidth requirement should be according to user needs.

Number of staff using computers	*Bandwidth in Mbps*		*Number of staff using computers*	*Bandwidth in Mbps*
1-10	2		121-140	28
11-20	4		141-160	32
21-30	6		162-180	36
31-40	8		181-200	40
41-50	10		201-240	48
51-60	12		241-280	56
61-70	14		281-320	64
71-80	16		321-360	72
81-90	18		361-400	80
91-100	20		Above 400	Individual case basis
101-120	24			

- **Physical network diagram:** should consider the number of users based on the organizational structure, interior design of the building and sitting arrangement (i.e. whether all users sit on same Floor or on different Floors)
- **Logical network diagram:** should take into account systems, service, and applications according to the institutional business processes.
  The physical and logical network infrastructure design in Government institutions should be put in four categories based on the number of users:

  - **Category 1:** Small-sized network infrastructure for up 30 users
  - **Category 2:** Medium-sized network infrastructure for up 50 users
  - **Category 3:** Large-size network infrastructure for about 100 users
  - **Category 4:** Network infrastructure for more than 100 users

- **Network security:** all government institutions should comply with the cybersecurity directives adopted in June 2018 for network and information systems.

Network Implementation

- Network equipment: network equipment and devices comprising the core network infrastructure to provide connectivity and security features include rack, minimum routers, switches, and access points, as well as a firewall.
- Network cabling, labeling and physical layout: any network structure should consider latest cabling and labeling standards.
- Communication room: institutions should have communication rooms at their premises when proven necessary and should comply with the following minimum requirements:

– ***Location***	The communication room at the institutional premises should be located in an isolated place and only be accessed by authorized people
– ***Size***	Minimum depending on the number of network equipment
– ***Temperature and humidity control***	Temperature to be maintained between, and air humidity must be controlled at level that is compliant with the equipment (17.7°C - 23.8°C, and 30%-55% for humidity)
– ***Structural consideration (floor, ceiling, and walls)***	The floor should be raised and well prepared to facilitate cleaning, cooling inside the room, and cabling installation, to allow elimination of dust. Floor tiles to facilitate cleaning Walls should have no external windows nor electrical conduits, should have wall block sensor, door frame size should be sufficient to allow easy removal of equipment, doors must open 180° outwards, minimum 90 cm wide and 2m high. Only equipment related to the communication room should be present in the room.
– ***Electrical system***	The communication room should have two different power source dedicated non-switched, power redundancy, supplies connected to UPSs on separate power circuits, a clear-labeled emergency power-off switch and monitor system. Should have automatic voltage regulator with circuit drawing and main switch board for all services, equipment grounding system and lighting rod. A regular maintenance and testing should be performed.
– ***Access control and safety***	Physical access to the communication room must be limited to only individuals with legitimate responsibilities justifying such access. Access control system (access card or biometric keyboard, or locking door) should be used at all entry points 24/7, and clear procedure to ensure access is removed when an individual no longer has entry permission, and access list must be reviewed periodically.
	Communication rooms should have fire prevention system, electric fire extinguishers and dry pipe fire suppression alarm system and CCTV cameras must be installed to monitor and record all events
– ***Communication room cabinet systems***	Racks enclosures should have at least adjustable 19U or 24U mounting rails, with access points for power and data pathways at the top and bottom. All cabinet must be lockable, and must be set in secure area within the Communication room.

In addition to the above minimum requirements, the following are guidelines for network equipment in the communication room:

− **Switches:** small medium and large institutions are advised to use 24 ports, PoE, 10/100/1000, 4 T/Small Form-Factor Pluggable (SFP) LAN Base image. A 48 ports switch may be used for larger institutions.
− **UTP data patch panels:** should be of CAT6, 24 ports or more depending on latest technology.
− **Routers:** should support high-bandwidth module-to-module communication at higher speeds based on the platform, some of the 10/100/1000 Ethernet ports can support small-form factor pluggable (SFP) based on connectivity in addition to RJ-45 connections, enabling fiber or copper connectivity.
− **Firewall:** latest firewall network security should be implemented. (For more details on requirements refer to Cyber Security directives)
Access Points: the number of access points may vary depending to the building configuration, advisable wireless standards are 802.11a/b/g/n/ac (2.4 GHz/5 GHz)
− **LAN Ethernet cabling:** CAT6 FTP or advanced types.

- **Documentation:** this includes network drawings, network connection and configuration information, addresses of all devices on the network with static IP addresses, and log documents. The document versions should be reviewed periodically, and any changes should be tracked.

Network Management

- Network performance: redundancy, load balancing, application response time, and quality of service should be controlled and assured.
- Network maintenance: each institution should elaborate a network maintenance plan, together with the disaster recovery and business continuity plan.