GOVERNMENT ICT STANDARDS

Government ICT Networks

ICTA.2.1.003:2023

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

© ICTA 2023 - All Rights Reserved

REVISION OF ICT STANDARDS

In order to keep abreast of progress in industry, ICT Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.

©ICT Authority 2023

Copyright. Users are reminded that by virtue of Section 25 of the Copyright Act, Cap. 12 of 2001 of the Laws of Kenya, copyright subsists in all ICT Standards and except as provided under Section 26 of this Act, no Standard produced by ICTA may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from the Chief Executive Officer.

ICT AUTHORITY (ICTA)

Telposta Towers 12th floor. Kenyatta Avenue P.O. Box 27150-00200, Nairobi Kenya Tel.: +254 20 2089061
Web:http://www.icta.go.ke
Email:standards@ict.go.ke

DOCUMENT CONTROL

Document Name:	Government ICT Networks
Prepared by:	Government ICT Networks Technical Committee
Edition:	Third Edition
Approved by:	Board of Directors
Date Approved:	3rd May 2023
Effective Date:	1st July 2023
Next Review Date:	After 3 years

CONTENTS

FOREWORD

The ICT Authority has the mandate to set and enforce ICT standards and guidelines across all aspects of information and communication technology including Systems, Infrastructure, Processes, Human Resources and Technology for the public service. The overall purpose of this mandate is to ensure coherent and unified approach to acquisition, deployment, management, and operation of ICTs across the public service in order to achieve secure, efficient, flexible, integrated, and cost-effective deployment and use of ICTs.

To achieve this mandate, the Authority established a standards committee to identify the relevant standard domains and oversee the standards development process. The committee consulted and researched broadly among subject matter experts to ensure conformity to acceptable international and national industry best practices as well as relevance to the Kenyan public service. The committee eventually adopted the Kenya Bureau of Standards (KEBS) format and procedure for standards development. In an engagement founded on a memorandum of understanding KEBS, participated in the development of these Standards, and gave invaluable advice and guidance.

For example, the ICT Networks Standard, which falls under the overall Government Enterprise Architecture (GEA), has therefore been prepared in accordance with KEBS standards development guidelines which are, in turn, based on the international best practices by standards development organizations including ISO.

The Authority's Directorate of Programmes and Standards has the oversight role and responsibility for management, enforcement, and review of this standard. The Directorate shall carry out quarterly audits in all the Ministries, Counties, Departments and Agencies (MCDA) to determine compliance to this Standard.

The Authority shall issue a certificate for compliance to agencies upon inspection and assessment of the level of compliance to the standard. For non-compliant agencies, a report detailing the extent of the deviation and the prevailing circumstances shall be tabled before the Standards Review Board who shall advise and make recommendations to remedy the shortfall.

The ICT Authority management, conscious of the central and core role that standards play in public service integration, fostering shared services and increasing value in ICT investments, shall prioritize the adoption of this standard by all Government agencies. The Authority therefore encourages agencies to adhere to this standard in order to obtain value from their ICT investments.

Stanley Kamanguya, OGW
Chief Executive Officer

1.0 INTRODUCTION

A network is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. Networks are components of the Government Enterprise Architecture (GEA) and constitute the infrastructure architecture layer. Networks are defined by the following aspects: the medium used to transport data, communications protocol used, scale, topology and the devices used to ensure efficient transfer of data from one point to another in the network.

Networks consists of, but not limited to, hubs, switches, routers, servers, Local Area Networks at the equipment locations, and Wide Area Links connecting sites together consisting of the coaxial cables, microwave and fiber optic equipment, and the network management tools provided by the equipment manufacturer.

In order to realize the Government Enterprise Architecture and to efficiently use network resources and realize its maximum benefits, it is important to provide a uniform framework for the design and configuration of the network and network devices.

Government network infrastructure (GNI) interconnects and provides internal MCDA connectivity. Government networks:

- Provide shared infrastructure services
- Provide a platform for shared services
- Facilitate data, multimedia and voice communication
- Reduce infrastructure development and managements Cost
- Remove/manage duplication
- Enable integration of future technologies
- Enable real time back up and disaster recovery services
- Provide a comprehensive security solution
- Facilitate conformity to International Standards

The, design, implementation and management of the Government Networks is guided by the following general principles that support the GEA:

- Be operational, reliable and available for essential business processes and mission-critical operations
- Provide for scalability and adaptability
- Use industry-proven, mainstream technologies based on open and pervasive-industry standards and open architecture
- Be designed with confidentiality and security of data as a high priority
- Allow secure remote accessibility
- Be designed to support converged services while accommodating data, voice and video services and to be "application aware" in the delivery of government services.

2.0 SCOPE

This ICTA Standard establishes guidelines for planning, design, implementation, utilization and management of network infrastructure in MCDA's single-tenant and multi-tenant buildings. The objective is to support the development and progressive growth of GNI in accordance with the Government Enterprise Architecture (GEA) principles.

3.0 APPLICATION

This standard will be applicable to the following:

- National Government of Kenya
- County Governments
- Constitutional Commisions
- State Corporations

4.0 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. All standards are subject to revision and, since any reference to a standard is deemed to be a reference to the latest edition of that standard, parties to agreements based on this standard are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below. Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards.

- ANSI/TIA-569-c
- ANSI/TIA-568-c.1
- ISO/IEC 60793
- IEEE, 802.3
- IEEE, 802.1
- IETF RFC 3457, 2709, 1518, 1918
- [ANSI/TIA-568-c.2]
- [ANSI/TIA-568-B.2.1]
- [IEEE 802.3af]
- [ANSI/TIA-568-C.3-1]
- [(ITU-T) Series G.652]
- [IEEE STD-- 802.3-2008]
- [IEEE 802.3an 2006]
- [TIA/EIA 568-B.3]
- [ISO/IEC 11801:2002]
- [ANSI/TIA-568-c.3]
- [IEEE STD-- 802.11-2012]

- [IEEE STD 802.11-2011]
- [IEEE 802.1x]
- [IEEE 802.11i, g]
- [ISO/IEC 17799:2005(E)]
- [IEEE 802.1Q]
- [ISO/IEC 17799:2000]
- [IEEE STD-- 802.3-2008]
- [IEEE 802.3an 2006]

5.0 DEFINITIONS

For the purposes of this ICTA Standard the following definitions, abbreviations and symbols apply:

5.1 Ad-hoc Network

Refers to a group of wireless devices communicating directly with each other (peer-to-peer or point-to-point) without the use of an access point or central server;

5.2 Aggregation network

Aggregation networks collect traffic from distribution networks and concentrate it onto high bandwidth facilities before they terminate on core or backbone networks;

5.3 Bridging

Connecting two different kinds of local networks, such as a wireless network to a wired Ethernet network;

5.4 Bluetooth

Describes how mobile phones, computers, and personal digital assistants (PDAs) can be easily interconnected using a short-range wireless connection;

5.5 CSMA/CA

Defined as Carrier Sense Multiple Access/Collision Avoidance, this is a method of data transfer used to prevent loss in a network;

5.6 Clear to Send

A Clear to Send signal is sent by a device to indicate its readiness to receive data;

5.7 Cabling Media

These include copper and optical fibre cabling;

5.8 Core Networks

Core networks provide the backbone for network services.

5.9 Demand Priority

Increases Ethernet data rate to 100 Mbps by controlling media utilization;

5.10 Delay

In a network based on packet switching, transmission delay (or store-and-forward delay, also known as packetization delay) is the amount of time required to push all the packet's bits into the wire. In other words, this is the delay caused by the data-rate of the link;

5.11 Extranets

An intranet or portion of an intranet to which an MCDA allows access by selected external entities, who could be partners of the MCDA;

5.12 Equipment room

The Equipment Room is the central point for telecommunications within the building. The Equipment Room is dedicated to the telecommunications function;

5.13 Entrance room

The telecommunications carriers (e.g. Telephone Company, ISP etc.) shall provide the point of demarcation for their services in the Entrance Room. The point of demarcation is analogous to a "border" between equipment and facilities owned by the carriers and that owned by the building occupants. Consequently, the Entrance Room will typically house terminations of copper and optical fibre cables (coming from outside the building) owned by the carriers. The Entrance Room is usually combined with a Common Equipment Room which houses electronic equipment owned by the carriers that is required to provide their network services;

5.14 Edge networks

Edge devices connect end users to the network;

5.15 Intranet

An intranet is a computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization;

5.16 Jitter

Jitter is any deviation in, or displacement of, the signal pulses in a high-frequency digital signal;

5.17 Logical Link

The logical link is the top sub-layer in the data-link layer, OSI Layer 2. It interfaces with the network Layer;

5.18 LAN

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, or office building.

5.19 Latency

Latency is a time interval between the transmission and reception of signal;

5.20 Metropolitan Area Network

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN);

5.21 Mesh Network

Extension of network coverage without increasing the transmit power or the receiver sensitivity;

5.23 Network Address Translation (NAT)

NAT technology translates IP addresses of a local area network to a different IP address for the Internet;

5.24 Network Monitoring and Management

Network monitoring is the use of a system that constantly monitors a network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages;

5.25 Path ways

Telecommunication pathways transport the cables.They include conduits, under floor ducts and floor boxes, raised floors, ceiling pathways, cable tray systems, perimeter pathways, telecommunication closet and equipment room;

5.26 Routing and Switching Technologies

Routing and switching ensure that computer connections and information flows do not breach the access control policy of the business applications;

5.27 Structured Cabling

Structured cabling is campus telecommunications cabling infrastructure that consists of a number of standardized smaller elements called subsystems e.g horizontal cabling wiring, back borne cabling wiring, telecommunication rooms, equipment rooms, work area components and entrance rooms;

5.28 TFTP

Trivial File Transfer Protocol (TFTP) is a version of the TCP/IP FTP protocol, which uses UDP (User Datagram Protocol). It has no directory or password capability;

5.29 Telecommunication path ways and spaces

This are cable trays, conduits and rooms that house and transport telecommunication cables for voice, data and electricity;

5.30 Token ring

This is a protocol that resides at the data link layer of the OSI model. It uses a special 3-byte frame called a ring that travels around the ring;

5.31 Telecommunications rooms

Telecommunications rooms are intended to distribute all telecommunications signals (e.g. voice, data, image) to the area they serve;

5.32 Through put

This refers to Percentage of data transmission per unit time.

5.33 User Datagram Protocol

User Datagram Protocol is a network protocol for transmitting data that does not require acknowledgement from the recipient;

5.34 Virtual Local Area Network (VLAN) Technologies

VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment. VLANs are usually associated with IP subnetworks; [IEEE 802.1Q]

5.35 Virtual Private Network

An IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium;

5.36 Voice over internet protocol

Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet;

5.37 Wireless Local Area Network

Wireless Local Area Network is a group of computers and associated devices that communicate with each other wirelessly;

5.38 Wi-fi

Wi-Fi is a local area wireless computer networking technology that allows electronic devices to network, mainly using the 2.4 gigahertz UHF and 5 gigahertz SHF ISM radio bands;

5.39 Wireless Personal Area Network

A network for interconnecting devices centered on an individual person's workspace - in which the connections are wireless;

5.40 Wireless Metropolitan Area Networks

A metropolitan area network (MAN) is a wireless computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area;

5.41 WAN

A wide area network (WAN) is a telecommunications network or computer network that extends over a large geographical distance;

5.42 Telecommunication Space

An area used for housing the installation and termination of telecommunications equipment and cable;

6.0 ABBREVIATIONS

ANSI American National Standards Institute
BGP Border Gateway Protocol
CoS Class of service
DHCP Dynamic Host Configuration Protocol
EMI Electro- Magnetic Interference
GEA Government Enterprise Architecture
GNI Government Network Infrastructure
ICT Information and Communication Technologies
IEEE Institute of Electrical and Electronics Engineers
IP Internet Protocol
ISO International Organization of Standardization
MBGP Multi-protocol Border Gateway Protocol
MCA Ministries, Counties and Agencies
MDAs Ministry, Departments and Agencies
MCDAs Ministry, Departments, Counties and Agencies
MGCP Multi gateway control protocol
MPLS Multi path label switching
NMS Network Sonitoring Software
OSPF Open Shortest Path Fast
PSTN Public Switched Telephone Network
RFC Request For Comments
RIP Routing Internet Protocol
RMON Remote Monitoring
SNMP Simple Network Management Protocol
SSH Secure Socket Shell
SSID Service Set Identifier
SSL Secure Socket Layer
TCP/IP Transport Communication Protocol/ Internet Protocol
TIA Telecommunications Industry Association
ToS Type of Service
UTP Unshielded Twisted Pair
VLAN Virtual Local Area Network
VOIP Voice over internet protocol
WPAN Wireless Personal Area Network

7.0 SUB DOMAINS

This section provides network standards needed to design, implement and manage Government Network Infrastructure. All MCDAs shall develop operational manuals to institutionalize the standards as per the sub domains below:

i. Telecommunication and Equipment path ways and spaces
ii. Structured Cabling
iii. Wireless Network Connectivity A) In controlled areas B) In public areas
iv. Fixed telephony service
v. Routing and Switching
vi. Network design, configuration, documentation and commissioning
vii. Internet
viii. Network Monitoring and Management
ix. Preventive Maintenance
x. Network security

8.0 STANDARDS REQUIREMENTS

8.0.1 Telecommunication Room, Pathways and Space

MCDA shall ensure Telecommunication Room, Pathways and Space should be properly designed and adaptable to change.The MCDA should have a separate telecommunication and equipment rooms. Each of the rooms shall adhere to the following standards.

8.0.2 Telecommunication Room Requirements

i. The size of the telecommunications room should be at least 71 square feet and there shall be no electrical distribution equipment in the room.
ii. A minimum of one meter should be provided for front, rear and side working access to the Cabinets.
iii. The size of the telecommunication room should be of sufficient to handle the cross connect field, associated electronic equipment, backbone and horizontal cabling and pathways. A minimum room size of 10 by 7 feet to serve 5000 square feet, a 10 by 9 to serve 8000 square feet, 10 by 11 feet to serve 10000 square feet of office space.
iv. Each government building shall contain at least one Floor Distribution room ranging from at least 13 by 13 feet and there shall be no electrical distribution equipment in the Floor Distribution rooms.
v. The size of telecommunication / equipment room in buildings with (> 300 cables) shall be a "walk in" design, i.e. capable of containing multiple standard cabinets.
vi. All MCDAs shall have an entrance room to provide the point of demarcation for their services in the Entrance Room.

8.0.3 Design

i. The door of the telecommunication/equipment room shall open outward, slide sideways, or be removable. It should be fitted with a lock and be a minimum of 36 inches wide by 80 inches high
ii. Sufficient lighting shall be provided. The light switches should be located near the entrance door. It is preferable for the rooms to be stacked vertically to facilitate running backbone cables through them.
iii. The telecommunication/equipment room shall be located in secure restricted area to which ICT personnel shall have 24-hour 7-day access. The room must be fitted with access control and CCTV surveillance in line with the current information security standards.
iv. The telecommunication/equipment room shall not have false(drop) ceilings and should be sufficiently separated from EMI sources such as antennas, medical equipment, elevators, motors and generators.
v. When a floor has more than one telecommunication/equipment room, standards also require that they be joined by a backbone pathway.
vi. Cable trays shall be used to lay cables instead of pulling them through a pipe.

vii. The telecommunication/equipment shall have a raised floor of not less than 300 mm with provisions for future expansion. several options for raised tiled server room floors, including:

- Concrete
- Cement
- Steel
- Vinyl and rubber

viii. MCDAs shall have an area for housing the installation and termination of telecommunications equipment and cables.

8.0.4 Environmental conditions

i. The telecommunication/equipment room shall be neat and devoid of any non telecommunication related components. The floor and walls should be sealed to inhibit dust ingress into the cabinets. Any openings should be sealed.
ii. Adequate ventilation should be provided by means of electric extractor fans and air inlets. In the larger installations (> 300 cables) the minimum requirement for air conditioning is a Heat Ventilation Air Conditioning (HVAC) System.
iii. The recommended temperature for telecommunications and equipment rooms is Cooling to a maximum temperature of 29 degrees celcius and a minimum temperature of 18 degrees. The temperature should not get colder than 10 degrees.
iv. Relative humidity should be maintained in the range from 30% to 80%.

8.0.5 Power

i. For telecommunication room electrical power shall be supplied by a minimum of two dedicated 220V-240V nominal from different phases, non-switched, AC-duplex electrical outlets. Each outlet should be on a separate branch circuits;
ii. Earthing and grounding shall be provided for both telecommunication and equipment room
iii. All telecommunication rooms should be equipped with electrical surge suppression and at least 2 SMART signaling UPSs that will supply the area with at least 8 hours of standby power in the event of commercial power failure. Provide standby lighting that will last for at least 6 hours if commercial power fails;

8.0.6 Pathways

a) Pathway Size

i. Trunking and cableways shall be sized at least 2.5 times the current installation requirements to provide for future expansion.

b) Pathway design

i. Cableways shall be completely separated from electrical power installations by a distance of 50 mm plus an earthed metal fillet.
ii. Cables should be enclosed within conduit or trunking.
iii. All installations, fixtures, fittings and structures disturbed during the installations must be reinstated to their original conditions.
iv. Metal powdered coated trunking shall be utilized; and other options can only be used where enviromental condition dictates. Metal powdered coated trunking size of a minimum of 50mm X 150mm dimension will be used.
v. All cables between MCDA buildings must be installed in ducting that complies with or is part of the approved Infrastructure plan in line with Fibre optic standard.
vi. Where set ceilings are used, sufficient easily removable ceiling access panels must be installed to allow future cable installation and removal.

8.1 Structured Cabling

8.1.1 Cabling media

a. Copper cabling

i. A work area shall have a minimum of two information-outlet ports. Each cable shall be assigned a unique cable number both at the patch panel and the data outlet. Wall plates shall be terminated with 8 pin modular jacks (RJ-45) and data outlets shall be flash mounted on metal trunking. There shall be no splicing of any cables installed. Intermediate cross connects transition points shall not allowed.

ii. Horizontal cabling should not terminate directly to an application specific device but rather to a telecommunication outlet. Horizontal Cabling infrastructure shall be done using minimum category 6A unshielded twisted-pair (UTP) cable for indoor and a minimum of Category 6 shielded twisted-pair(STP) for outdoor.

iii. Patch cords used in the horizontal Cabling, including equipment cables/cords, should not exceed 5m. Horizontal cable between the face plate and the patch panel shall not exceed 90m.
iv. Connectors shall be protected from physical damage and moisture.

8.1.2 Cabinet

a. Cabinet Size

i. In installations less than or equal to 200 data points, at least one cabinet with a minimum of 42U full height good quality shall be used. In installations greater than 300 data points, additional cabinets of a minimum of 22U floor standing cabinet or 19U wall mounted cabinet located in a suitable closet shall be used.

b. Cabinet Design

i. Each cabinet should be identified by using an agreed name (a, b, c, d , etc) or as on services drawing.
ii. Each cabinet should contain a rack mountable power distribution unit, installed with one 3 pin power outlet per 24 user data points.
iii. A Cables shall be terminated in RJ45 19 inch Patch panels. All rising cables should be on a tray outside the 19 inch rack space and a shelf should be installed to protect the cables in the bottom of the cabinet in the case of floor standing cabinet.
iv. Each data patch panel should be identified by a, b, c, and d from the top of the cabinet. The number on the cabinet should be used for identification. On a 1 to 24 way panel, the maximum number should be 24 and on a 1 to 48 way panel, the max number should be 48. For example, BA-A-01 would represent Block A Patch panel A point number 1.
v. All cabinets must have a forced cooling. Each cabinet should be equipped with a roof mounted 4 fan cooling fan tray. In smaller installations electric A.C. fans should be placed in the cabinet to keep the active components cool.

c. Cable Security

i. Network cabling should be protected from unauthorized interception or damage using a conduit / duct.
ii. For sensitive or critical systems further controls to consider shall be considered that include armoured conduit and locked rooms or boxes at inspection and termination points, use of alternative routings and/or transmission media providing appropriate security, electromagnetic shielding should be used to protect the cables and control access to patch panels and cable rooms.

8.2 Wireless Network Connectivity

8.2.A Wireless Network Connectivity in controlled areas

The following shall be in line with GoK information security standards

i. Wireless network installation shall be authenticated between wireless clients and access points to ensure that clients do not connect to a rogue access point deployed by an attacker. This would also
ensure that un-authorized wireless users do not connect to the MCDA's wireless networks.
ii. Sensitive data between wireless clients and access points should be protected using encryption.
iii. Use of Network ID (SSID) and enforcement of MAC Address Filtering shall be used to secure wireless network and enforce.
iv. WPA2 shall be used as bare minimum security for authentication and protection of information on a wireless local area network (WLAN).
v. Government organizations shall change the keys/secrets associated with the wireless access points at least once in six months through a managed process.
vi. Government organizations shall periodically, as defined by the MCDA security policy, scan for unauthorised wireless access points and take appropriate action if such access points are discovered. The scan should not be limited to only those areas containing the high-impact information systems, but should also cover the adjacent areas.
vii. A guest VLAN shall be created for all guests to access internet only.
viii. Wireless networks should be reviewed from time to time to ensure that obsolete networks are retired and up-to-date networks installed that meets the performance requirements.

8.2.B Wireless Network Connectivity in public areas

The following shall be in line with GoK information security standards

i. Wireless network installation shall be authenticated between wireless clients and access points to ensure that clients do not connect to a rogue access point deployed by an attacker. This would also ensure that un-authorized wireless users do not connect to the public wireless networks. Minimum authentication requirements shall include full names ,National ID number and registered mobile number.
ii. Sensitive data between wireless clients and access points shall be protected using encryption.
iii. Use of Network ID (SSID) and enforcement of MAC Address Filtering shall be used to secure wireless network and enforce.
iv. WPA2 shall be used as bare minimum security for authentication and protection of information on a wireless local area network (WLAN).

v. Government organizations shall periodically, as defined by the MCDA security policy, scan for unauthorised wireless access points and take appropriate action if such access points are discovered. The scan should not be limited to only those areas containing the high-impact information systems, but should also cover the adjacent areas.
vi. Wireless networks should be reviewed from time to time to ensure that obsolete networks are retired and up-to-date networks installed that meets the performance requirements.
vii. All access points must be mounted and grilled on a secure area of a minimum height of 6M.

8.3 Fixed telephony service

8.3.1 VOIP service type selection

i. MCDAs shall implement VOIP service for their organization that can be either of the following VOIP service types and their applications: Integrated access service, SIP trunks , Managed IP PBX , Hosted IP PBX.

8.3.2 VOIP software

i. Software selection shall include: call by name, caller ID, last number redial, hold, call waiting, call forwarding , transfer, divert, park, retrieve, voice mail, return call and call conferencing and support Local Number portability.

8.3.3 VOIP deployment

i. MCDAs shall endeavor to integrate VOIP with existing telephone infrastructure
ii. MCDAs shall separate voice and data traffic logically on the network (using VLANs)
iii. MCDAs shall ensure use of PoE switches to power the telephones
iv. Cabling shall be CAT 6 or higher
v. Network cards of the VOIP devices shall be running at a minimum of 100Mbps, fast ethernet
vi. MCDAs shall incoporate Service level agreement, User training, Support, Future growth when selecting a service provider for VOIP.
vii. MCDAs shall maintain an up to date Telephone Directory and Call history log.

8.4 Routing and Switching

i. MCDAs shall have switching and routing devices to provide network access to the computing enviroment.
ii. The switching devices shall have an autosensing of 100/1000Mb/s, minimum managed 24 port for connection to the horizontal cabling.
iii. The switching device shall be rack mountable, support IP routing, Quality of Service(QoS) and Power over Ethernet (POE).
iv. The routing devices shall be manageable and have a minimum of 1000Mb/s, minimum 4 ports, rack mountable, support advanced IP routing, Quality of Service(QoS).

8.5 Network design, configuration, documentation and Commissioning

i. MCDA shall carry out site surveys to ensure a network design that guarantees maximum service availability
ii. MCDA shall develop a network design with associated specifications and Bill of Quantites (BoQ)
iii. MCDA shall ensure that relevant functionalities are installed and configured to deliver robust and secure IP network.
iv. Upon completion of the installation and configuration MCA shall carry out the tests and the results recorded in one or several measure books showing test results of the cable components.
v. MCDA shall ensure that physical and logical design of the network is documented 'as built'. The documentation shall also include; Synopsis of the cabling (primary and secondary), Charts of the distribution highlighting the details of the elements that have been installed, Detailed map of socket layout and Reports on measurements.
vi. All components shall be tested and a Completion Certificate issued.
vii. Physical and logical designs shall be updated whenever changes occur.

8.6 Internet

i. MCDA shall ensure that internet bandwidth is 10 Mbs minimum for the users needs.
ii. Internet service availability shall be at least 99.99 %
iii. MCDA shall sign and enforce a service level agreement with the Internet Service Provider (ISP) to guarantee 99.99% availability.
iv. MCDA shall assign internal workstation network IP address using Dynamic Host Configuration Protocol (DHCP).
v. MCDA shall use subnetting to protect IPv4 / IPv6 spaces as may be applicable.
vi. MCDA shall ensure redundancy for internet connectivity for high availability
vii. MCDA shall develop and sensitize users on acceptable internet usage policy
viii. MCDA occupying or moving to new offices shall ensure that the offices are internet ready.

8.7 Network monitoring and management

i. MCDA's shall acquire an appropriate monitoring and management tool / software. The tool shall have capability to; Discover network components such as devices and links, Support Layer 2 and Layer 3 discovery, Generate a layout of the existing network, Report failures and event logs, Receive SNMP trap messages and Generate customized reports as minimum features.
ii. MCDA shall ensure that network monitoring and management role of the staff is defined.
iii. MCDA shall ensure that usage and utilization of bandwidth is controlled using appropriate bandwidth management tools, or traffic or packet shapers.
iv. MCDA shall Configure SNMPV3 on network devices. A VLAN shall be dedicated for management purposes and shall not be used to forward traffic externally. Remote access shall be through a VPN and NAT functionality which must be enabled.
v. MCDA shall ensure Service Level Agreements (SLAs) are maintained with a minimum of WLAN, WAN and internet service availability of 99.99%
vi. MCDA shall specify the mean time to failure (MTTF) for all replaceable devices using acceptable methods for predicting the failure for electronic equipment (IEC/TR 62380)
vii. MCDA shall ensure network throughtput of 100% with line rate equal to 100% maintained. latency of less than; 130 µs for a 1518 byte frame on a 100 Mb/s ethernet interface, 18 µs for a 1518 byte frame on a 1 Gb/s ethernet interface and 6.5 µs for a 1518 byte frame on a 10 Gb/s ethernet interface.

8.8 Preventive maintenance (PM)

i. Maintenance programs shall be identified to detect imminent or conditional failures such as thresholds for CPU and memory, interface utilisation and errors, temperature, power supply current and voltage.
ii. Maintenance programs shall be identified for all assets to ensure that the hardware, firmware, software, physical and logical configuration is as designed throughout the life of the asset.
iii. All message logs with a severity level between 0 and 4 inclusive as defined in IETF RFC 5424 shall be logged to syslog.
iv. All message logs with a severity level between 0 and 2 inclusive as defined in IETF RFC 5424 shall be regarded as failures requiring immediate corrective action.
v. All message logs with a severity level of 3 or 4 as defined in IETF RFC 5424 shall be regarded as conditional failures requiring priority preventative action.
vi. Preventive and maintenance shall be carried out quartely.
vii. Corrective Maitenance shall be done on need basis.

8.9 Network Security

MCDA shall ensure the following are configured in line with GoK information security standards

i. VLANs - Firewall and Perimeter Security Architecture
ii. Connections to Third Parties
iii. Remote Network Administration to Servers

iv. Encryption of Sensitive Information
v. Virus Protection
vi. E-mail Security
vii. Wireless Security Management
viii. Redundancy of Network Infrastructure
ix. Auditing and Monitoring of Security Logs
x. Network Intrusion Detection - Network Segmentations
xi. Segregation of Duties
xii. Default User IDs and Network Device Configuration
xiii. Network Inventory and Asset Management
xiv. Network Configuration Management
xv. Vulnerability and Patch Maintenance.

i. APPENDIX I: TEMPLATE FOR NETWORK INSPECTION IN PREPARATION FOR COMMISSIONING

TENDER NO: **CONTRACTOR:** **DATE:**

ITEM	DETAILS	YES/NO	REMARKS
Serial Numbers and Models of Switches indicated in Final Documentation	Switches		
	UPSs		
	Routers		
	DTU		
Brief Description of Project Details	-		
Network Layout Diagram	Data Points Labelled		
	Positions of Cabinets on Floors Indicated		
	New Trunking Installed Indicated		
	Fibre Optic Backbone Diagram		
	Site Layout Diagram		
Test Results	Test Result Matching Data Points		
	Data Points Matching the Design		
	Summary of Data Points Per Cabinet		
	Confirm lengths of cables relative to cabinet positions		
	Test Results for Fibre Cables		
Confirmation of detailed gathered in field against the documentation.			
Ready for commissioning			

Name: **Sign:** _____

Name: **Sign:** _____

ii. APPENDIX II: INSPECTION CHECKLIST FOR COMPLETED PROJECTS FOR FINAL INSPECTION

TENDER NO: **CONTRACTOR:** **DATE:**

	FLOOR				
1.	Location				
2.	Cabinet Size				
3.	**Check Earthing of Cabinet**				
4.	**Copper Patch Panels**				
	Make of copper panels				
	No of 24 port on copper panel				
	No of 48 port on copper panel				
	No of terminated ports on copper panels				
	Category of copper patch panels (Cat 6?)				
	No of Cable Managers				
	No of 3m Patch Chords				
5.	**Fibre Optic Patch Panels (where applicable)**				
	Make of Patch Panel				
	No of Fibre Optic patch panels				
	Make of Fibre Optic panels				
	No of ports on Fibre Optic panel				
	No of terminated ports on Fibre Optic panel				
6.	**Patch Chords (User Area)**				
	Total No of 5m Patch Chords				
	Total No of 3m Patch Chords				
7.	**UTP Cables used**				
	Category of cables				
	Make of cables				
8.	**LAN edge Switches Serial Nos**				
	Type of switches (Make and Model)				
	No of 12 port of switches				
	No of 24 port of switches				
	No of 48 port of switches				
	No of GigaEthernet ports connected				

	FLOOR				
9.	**Core Switch Serial No (where applicable)**				
	Type of switch (Make and Model)				
	No of Power Supply Units (PSU)				
	Power Capacity of PSU				
	No of GigaEthernet modules				
	No. & Type of Supervisor Engines				
	No. & Type of Gigabit Line Cards				
10.	**Type of UPS (Make and Model)**				
	UPS Serial/Nos.				
11.	**DTU Serial Number**				
12.	**Router Serial Number**				

Name: **Sign:** _____

Name: **Sign:** _____

iii. APPENDIX III: PROGRESS OF JOBS PER SITE – THIS IS FOR PROJECTS STILL NOT COMPLETE

TENDER NO: **CONTRACTOR:** **DATE:**

	ACTIVITY	DETAILS REQUIRED	COMMENTS
1.	Site Visit	(Y/N)	
2.	Installation of Trunking	% Done	
3.	Installation of Cabinets	% Done	
4.	Earthing of Cabinets	% Done	
5.	Pulling of UTP cables	% Done	
6.	Termination of UTP cables	% Done	
7.	Pulling of Fibre Optic cables	% Done	Where Applicable
8.	Termination of Fibre Optic cables	% Done	Where Applicable
9.	Testing of UTP cables	% Done	
10.	Testing of Fibre Optic Cables	% Done	Where Applicable
11.	Labeling of patch panels	% Done	
12	Labeling of data points	% Done	
13	Installation of Switches	% Done	
14	Installation of DTU	(Y/N)	
15	Installation of Router	(Y/N)	
16	Installation of UPSs	% Done	
17	Repair of Damages	(Y/N)	
18	Ready for Commissioning	(Y/N)	
19	Documentation Ready	(Y/N)	

Name: **Sign:** _____

Name: **Sign:** _____

ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
t: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: @ICTAuthorityKE


ICT
Authority