GOVERNMENT ICT STANDARDS

Public Wi-Fi Standard

ICTA.2.1.005:2025

First Edition 2025

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

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 (ICTA)

Head Office: P.O. Box 27150, Nairobi-00100, Tel.: (+254 202) 211 960/61
E-Mail: standards@ict.go.ke, Web: http://standards.icta.go.ke

DOCUMENT CONTROL

Document Name:	Public Wi-fi Standard
Prepared by:	Government Public Wi-fi Technical Committee
Edition:	First Edition
Approved by:	Board of Directors
Date Approved:	7th August 2025
Effective Date:	7th August 2025
Next Review Date:	After 3 years

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. The Electronic Records Management Standard, which falls under the overall Government Enterprise Architecture (GEA), has therefore been prepared in accordance with KEBS standards development guidelines based on the international best practices by standards development organizations including International Organization for standardization (ISO). The ICT Authority in consultation with Kenya National Archives and documentation Service has the oversight role and responsibility for management, enforcement and review of this standard. The Ministries, Departments, Agencies and Counties will be audited annually to determine compliance. 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. 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.

Zilpher A. Owiti, OGW
Ag. Chief Executive Officer
ICT Authority

CONTENTS

1.0 INTRODUCTION

The Government of Kenya (GoK), through its commitment in Kenya's National Digital Masterplan 2022-2032, intends to expand digital access and promote inclusivity. Some of the initiatives envisaged in the digital master plan include deployment of 25,000 public Wi-Fi hotspots, set up of digital hubs, and rollout of 100,000 kilometers of fiber network. The public Wi-Fi hotspots initiative is aimed at enhancing connectivity for citizens across the country.

Public Wi-Fi hotspots will be deployed in common public spaces, including but not limited to;

i. Markets
ii. Bus station and Boda-boda shades
iii. Parks,
iv. Stadiums
v. Training centers and learning institutions
vi. Postal Office
vii. Trading centers
viii. Digital Hubs

This standard has been developed to guide the design, deployment, and management of public Wi-Fi infrastructure. It outlines requirements to ensure that public Wi-Fi networks are secure, reliable, and uphold the quality of service.

To ensure that value is realized from the deployment of public Wi-Fi hotspots, the end-to-end process has to adhere to GoK ICT Networks and Information Security. The public Wi-Fi initiative seeks to reduce the digital divide to improve access to digital services and bolster e-commerce, it presents numerous challenges related to quality of service, cyber threats, and sustainability. Thus, this standard will serve to ensure:

- Reliable and efficient connectivity to the target beneficiaries
- Safe and secure access to the internet and related services
- Longevity and cost-effective maintenance of the Public Wi-Fi Infrastructure

2.0 SCOPE

This standard sets out the minimum requirements for the design, deployment, and management of public Wi-Fi.

3.0 APPLICATION

This standard applies to Ministries, State Departments, Agencies, and Counties (MDACs) involved in the design, deployment and management of public Wi-Fi.

4.0 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions on the standard;

i. IEEE 802.11x: wireless networking standard, 2001
ii. Wi-Fi Protected Access standard (WPA), 2018 WPA3
iii. Government of Kenya ICT network standard,2023
iv. Government of Kenya Information Security Standard, 2023
v. KS ISO/IEC 27001:2022 – Information-Security Management System
vi. KS 29-52 Accessibility standards for persons with disability
vii. Computer misuse and cybercrime Act
viii. General Data Protection Regulation (GDPR)
ix. Health Insurance Portability and Accountability Act (HIPAA)
x. Kenya Information and Communications Act (KICA)

5.0 DEFINITIONS

For the purposes of this Standard, the following definitions shall apply:

5.1 AP – Access Point

A network device that allows wireless-capable devices (like laptops, smartphones, and tablets) to connect to a wired network using Wi-Fi (IEEE 802.11 standards).

5.2 Bandwidth Throttling

Intentional slowing of internet throughput for certain users or services, implemented to manage network performance and ensure fair usage.

5.3 Captive Portal

A network access control mechanism that redirects a user's web browser to a specific login or information page, usually required to be completed before internet access is allowed, often used in public wireless networks.

5.4 Carrier capacity

The maximum amount of data or traffic load that a network carrier (such as an Internet Service Provider or telecommunications operator) can transmit through its infrastructure over a given time. It is typically measured in bits per second (bps), such as Mbps, Gbps, or Tbps.

5.5 Carriage Service Provider (CSP)

A licensed telecommunications carrier or network service provider that provides network connectivity services.

5.6 Client roaming

The process where a Wi-Fi enabled device (the client) seamlessly transitions its connection from one access point (AP) to another within the same wireless network (same SSID) without a noticeable interruption in service for the user.

5.7 Client Identity Management (CIDM)
A government system and policy for consistent registration, authentication, and management of users' identities when accessing government digital services. CIDM integration.

5.8 Connectivity Plan
outlines how devices, systems, and users will be connected to a network to ensure reliable, secure, and scalable access to internet and digital services. In the context of Public Wi-Fi deployment, a well-structured connectivity plan is crucial to guide infrastructure, topology, bandwidth, and service continuity

5.9 Content Filtering
Mechanism of restricting or blocking access to certain online content deemed unauthorized, offensive, or harmful, based on predefined policies.

5.10 Environmental and Social Impact Assessment (ESIA)
Systematic process used to evaluate the potential environmental and social effects of a project, particularly in IT-related developments.

5.11 IP Address Management (IPAM)
systematic approach to managing and tracking IP address allocations and configurations within a network

5.12 Internet Protocol (IP)
Fundamental protocol in the Internet Protocol Suite, which is responsible for addressing and routing packets of data so that they can travel across networks and reach their intended destinations.

5.13 Fiber
High-speed data transmission medium that uses light signals to carry information over long distances through thin strands of glass or plastic.

5.14 Internet Protocol (IP)
The fundamental set of rules used for sending and receiving data across digital networks. Power over Ethernet (PoE)

5.15 Jitter
Refers to the variation in the delay of received data packets over time.

5.16 Layer 2
Refers to the Data Link Layer in the OSI (Open Systems Interconnection) model. It handles framing, addressing, error detection, and flow control, ensuring efficient and reliable data transfer.

5.17 Layer 3
Refers to the Network Layer in the OSI (Open Systems Interconnection) model. It facilitates the routing of data packets between devices across different networks.

5.18 Network Management System (NMS)
Software application or suite of applications used to monitor, manage, and maintain computer networks

5.19 Packet loss
Defined by when data packets traveling across a digital network don't make it to their intended destination.

5.20 Service Level Agreement (SLA)
It is a contractual agreement or a documented understanding between a service provider (internal or external) and a client (end-user, department, or another company) that defines the scope, quality, and terms of the IT services being provided.

5.21 Virtual Local Area Network (VLAN)
Networking technology that allows network administrators to create logically segmented networks within a physical network infrastructure.

5.22 Virtual Routing and Forwarding (VRF)
Technology used in networking that allows multiple instances of a routing table to coexist on the same router or switch.

5.23 Public Wi-Fi
A wireless Internet access service offered to the general public provided within public spaces or government facilities. Public Wi-Fi in this context is a government-provided service intended for use by citizens.

5.24 Satellite
Used to transmit and receive signals for voice, video, and data communication over long distances.

5.25 Session Time
The defined duration a user is allowed to remain connected to the public Wi-Fi network in one continuous session.

5.26 Splash Page
A captive portal webpage that is presented to users when they first connect to the public Wi-Fi.

5.27 Terms and Conditions of Use
The formal agreement or rules that outline the user's rights and responsibilities when accessing the public Wi-Fi service, as well as the disclaimers and obligations of the provider.

5.28 Throughput
The actual amount of data successfully transmitted over a network from one point to another within a given time frame, typically measured in bits per second (bps), such as Mbps (Megabits per second) or Gbps (Gigabits per second).

5.29 Quality of Service
a set of technologies and mechanisms that manage and prioritize network traffic to ensure a reliable and predictable performance for specific applications and services.

5.30 Walk test

Methodical process of physically walking through the intended coverage area of the wireless network while actively using a wireless client device to assess the signal strength, coverage, performance, and roaming capabilities of the network.

5.31 Wireless Fidelity (Wi-Fi)

Wireless networking technology that uses radio waves to provide wireless Internet access

6.0 ABBREVIATIONS

AP Access Point
CIA Confidentiality, Integrity & Availability
CIDM Client Identity Management
CMCA Computer Misuse and Cybercrimes Act
CRQ Change Request
CSP Carriage Service Provider
ESIA Environmental and social impact assessment
FTP File Transfer Protocol
FUP Fair Usage Policy
GEA Government Enterprise Architecture
GoK Government of Kenya
HTTP Hypertext Transfer Protocol
HTTPS Hypertext Transfer Protocol Secure (SSL/TLS)
ICT Information and Communications Technology
ICTA ICT Authority
IP Internet Protocol (address)
IPAM IP Address Management
KEBS Kenya Bureau of Standards
MAC Media Access Control (address)
NMS Network Management System
ODPC Office of the Data Protection Commissioner
PoE Power over Ethernet
SLA Service Level Agreement
VPN Virtual Private Network
VRF Virtual Routing and Forwarding
VLAN Virtual Local Area Network
GDPR General Data Protection Regulation
HIPAA Health Insurance Portability and Accountability Act of 1996 (U.S. law)
KICA Kenya Information and Communications Act (KICA)

7.0 SUB DOMAIN

This standard cover;

i. Planning and Design
ii. Deployment
iii. Quality of service
iv. Maintenance and support
v. Public Security
vi. Power

Requirements

7.1 Planning and Design

7.1.1 The responsible entity shall undertake and document High-level and Low-level site surveys. The survey shall take into consideration;

i. Environmental and social and environmental impact (ESIA).
ii. Site bandwidth demand and service area population
iii. Number and positioning of access points (APs)
iv. Proposed location of centralized/decentralized or cloud-based wireless controllers
v. Switch needed for optimal bandwidth distribution and monitoring (at least Layer 3 and Managed switch or router)
vi. Sustainable/Reliable power
vii. The appropriate topology
viii. Redundancy, fault tolerance, and future upgradability/scalability.

7.1.2 The detailed design shall include:

i. Connectivity plan
ii. Operators (internet service provider/ network)
iii. Base transceiver stations
iv. Access points distribution on LAN,
v. Source site's name and equipment models
vi. Interception maintenance chamber (manhole) and handhole positions
vii. Link budgets
viii. Splice points with tube and core numbers
ix. Network elements
x. Wi-Fi signal coverage.

7.1.3 Technical design shall be prepared and subjected to technical reviews. The output of the design process shall include;

i. Detailed engineering drawings for both physical, rack/cabinet layout and logical with fiber route maps (KMZ/ KML and PDF files)
ii. Link budget calculations
iii. Bill of quantities (BoQ) and materials specification
iv. Risk assessment and mitigation plan
v. Construction and implementation schedule
vi. Compliance checklist
vii. GIS mapping and /or structured drawings for both physical and logical layers

7.1.4 Stakeholders shall be engaged on Wayleave applications, environmental and social impact assessments (ESIA), and any other associated regulatory approvals before final sign-off of designs.
7.1.5 The design documents shall be duly approved before implementation.
7.1.6 Any deviations from approved design shall be duly approved.
7.1.7 Network designs shall incorporate reliability-enhancing systems for critical equipment and, where feasible, redundant connectivity links at high-priority sites.
7.1.8 Public Wi-Fi equipment shall conform to the minimum specifications provided on Annex I

7.2. Deployment

7.2.1 Deployment of Local Area Network (LAN) Installations shall be in accordance with the GoK ICT Network Standard
7.2.2 All Access points shall be powered by Power Over Ethernet (POE) switch.
7.2.3 Centralized controllers shall be installed in the appropriate proposed locations.
7.2.4 For Indoor cabling, all cables shall run on a standard powder-coated metallic trunking
7.2.5 All sites shall have an IP addressing plan
7.2.6 The IP addressing plan shall be well documented or recorded in IP Address Management System (IPAM)
7.2.7 Proper network segmentations shall be implemented using VLANs or Virtual Routing and Forwarding (VRF), as required.
7.2.8 Site configurations shall adhere to the appropriate activation model—either Layer 2 or Layer 3— to ensure optimal quality of service
7.2.9 Centralized or cloud-based wireless controllers shall be properly configured to ensure visibility and reachability to all deployed access points.
7.2.10 Comprehensive testing shall be conducted to verify that all wireless parameters—such as SSID configuration, security protocols (including WPA3), and captive portal functionality—are correctly implemented.
7.2.11 Pre-walk test and post walk tests shall be conducted and implement the necessary interventions.
7.2.12 All Switches and routers shall be onboarded to a centralized network monitoring tool (NMS) and tested.
7.2.13 Inspection and Acceptance of deployed public Wi-Fi sites shall be guided by an approved checklist.
7.2.14 Quality checks shall be conducted after configuration and site activations to ensure compliance with the defined service level standards. This shall include, but is not limited to,
i. Weekly speed tests
ii. User satisfaction assessments
iii. Automated monitoring of network uptime
iv. Device performance,
v. Overall system health

7.3 Service Quality and Performance

7.3.1 Tools for QoS and Performance Monitoring shall be deployed and maintained
7.3.2 The following Quality of Service (QoS) mechanisms shall be configured and tested;
i. Traffic Classification
ii. Bandwidth Control & Rate Limiting:
iii. Application-Based Prioritization:
iv. Prioritize essential services.
v. Service Differentiation:
vi. Congestion Management:

7.3.3 The following Network health indicators shall apply;

S/No	Parameter	Description	Indicator
1.	Throughput	The actual speed users experience should meet or exceed defined service-level targets	≥5 Mbps /user
2.	Latency	Delay in packet delivery;	(less than) <100 MS for interactive applications
3.	Jitter	Variation in packet delay; important for real-time services	(less than) <30 Ms.
4.	Packet Loss	Percentage of dropped packets.	(less than) < 1% for most services.
5.	Client Roaming & Session Continuity	Seamless handoff between APs without disconnection	
6.	Uptime & Availability	Target	>99% availability with power backup and failover links

7.4 Maintenance and support

7.4.1 A Service Level Agreement shall be developed and monitored for support and maintenance of public Wi-Fi sites.
7.4.2 Preventive maintenance plan shall be developed and implemented.
7.4.3 The network shall be continuously monitored through NOC/SOC.
7.4.4 Usage reports, fault logs, and service availability shall be prepared and retained.
7.4.5 Quarterly site audits shall be undertaken to verify equipment status, site security compliance, and service levels that is ICTA to enforce within MDACs; CA to enforce across industry/private sector.
7.4.6 Performance trends shall be reviewed to guide future upgrades or expansions.
7.4.7 An up-to-date inventory of public Wi-Fi equipment shall be maintained

7.4.8 Disaster recovery, the following are disaster recovery procedures;
i. Assess the outage (hardware failure, cyberattack, or power issue).
ii. Switch to backup systems (secondary ISP, backup AP controller, failover power).
iii. Restore configurations from backup if equipment fails.
iv. Verify network integrity (ping tests, bandwidth tests, captive portal login).
v. Gradual restoration →bring services up in phases (core →distribution →APs).

7.5 Public Wi-Fi Security

7.5.1 The following Security measures shall be configured:
i. Captive Portal with Authentication
ii. Privacy-by-design e.g. Role-Based Access Control (RBAC), (ISO 27001, GDPR).
iii. Media Access Control (MAC) Address Filtering:
iv. Secure Wireless Protocols WPA3
v. Use strong encryption standards with 802.1X authentication (RADIUS-backed).
vi. Disable Open Networks Without Encryption:
vii. Traffic Segmentation and Isolation: Client Isolation, Network Segmentation, and Firewall Filtering
viii. Content Filtering and Threat Protection
ix. Intrusion Detection and Prevention (IDS/IPS)

7.5.2 Default passwords shall be changed on all devices; use complex, regularly updated credentials.
7.5.3 Network devices shall be kept up to date on security patches.
7.5.4 Unused and insecure services shall be disabled

7.5.5 Compliance with Data Protection Laws shall be enforced as follows;
i. Display clear terms of service and privacy policy on the captive portal with a checkbox for user consent.
7.5.6 Engagement of third parties licensed by ODPC on data protection

7.6 Power

7.6.1 Proper power capacity planning shall be done to determine power requirement based on the public Wi-Fi site load
7.6.2 All public Wi-Fi Sites shall be connected to a stable and clean national grid power or green power based on equipment load needs
7.6.3 Surge protection and grounding systems shall be put in place.
7.6.4 All public Wi-Fi equipment shall draw power through a secure and dedicated power breaker module to ensure safety, protection, and controlled power distribution
7.6.5 Backup solutions shall be used to ensure Public Wi-Fi site reliability and availability during national grid power outages

8.0 ANNEXES

Annex 1
Equipment

1. Routers

Requirement	Specifications
General requirements	Equipment must be carrier-grade, suitable for core or aggregation network, support scalable port options, be designed for high availability, redundancy and modular scalability, compliance with industry standards, capable of IPv4/IPv6 dual stack, support SDN (Software Defined Networks) and programmable interfaces. In addition, the equipment must support forward and backward compatibility and is able to integrate with existing networks.
Hardware requirements	Equipment must have a modular chassis-based system with hot-swappable components, redundant supplies and fans, front-to-back/ side-to-side airflow options, support non-blocking architecture and high-speed backplane. The interfaces and inline cards should support multiple interfaces types, auto-negotiation and port bonding (LACP) and Zero-touch provisioning (ZTP).
Routing and Protocols	Equipment must support layer 2 features such as VLAN, Link aggregation, Ethernet OAM and MPLS for VPNs and traffic engineering; layer 3 features such as static routing, OSPF, IS-IS, BGP-4, IPv4 and IPv6 full internet table, virtual routing and forwarding (VRF) and segment routing (SR-MPLS, SRv6) capability and support high availability and redundancy via Non-Stop Forwarding (NSF), Graceful Restart (GR), Bidirectional Forward Detection (BFD) and multi-chassis clustering or virtualization.
Traffic Management and Security	Equipment must support QoS (Classification, policing, shaping, scheduling), Access Control Lists (ACL)for security and traffic filtering and DDoS protection and Control Plane Policing, MACsec/IPsec support for encryption.
Management and Monitoring	Equipment must support global industry management interfaces such as CLI, Web GUI, and API (NETCONF, RESTCONF, gNMI), SNMPv2/v3, Syslog, Telemetry, sFlow, NetFlow/IPFIX; integration with NMS/OSS platforms and redundant management interface (Ethernet/Console/ USB)
Compliance and Certification	Equipment must be compliant to relevant industry standards and certifications

2. Switches

Requirement	Specifications
General requirements	Equipment must be enterprise-grade, carrier-class or datacenter switch, depending on use case, fixed or modular chassis design support for scalability and redundancy compliance with industry standards and support SDN (Software Defined Networks) with APIs such as OpenFlow, NTECONF, RESTCONF,gNMI APIs, . In addition, the equipment must support forward and backward compatibility and is able to integrate with existing networks
Hardware Specifications	Equipment shall be rack mountable or stackable and support front-to-back or side-to-side airflow options. Access Switch: Support 1G/2.5G/5G/10G Base-T (RJ-45) or SFP/SFP+ fiber ports and at least 2x10G/25G uplink ports Aggregation Switch: Support 10G SFP+ fiber ports and 2 to 4 ports of 40/100G uplinks and support multi-gigabit Ethernet auto-negotiation
Core Switch	Support 32 or 64 ports of 10G/25G/40G/100G/400G, modular chassis, support multi-chassis or VSS (Virtual Switching System) and up to 8 switches in a stack with more than 480 Gbps backplane bandwidth.
Switching and Routing Capabilities:	Layer 2 and Layer 3 Support: Support industry features for Layer 2 and layer 3 such as VLANs, Link aggregation, STP Support, Ethernet OAM, carrier-grade deployment, PIv4/IPv6 routing, network segmentation, policy-based routing, fast failure recovery and load balancing.
Security and Traffic Management:	Support industry features such as routing and integration, data encryption, filtering and traffic security, DHCP Snooping, ARP inspection, IP Source Guard, Storm control, broadcast/multicast suppression and QoS.
Network and Management Features	Support industry features such as consoles, real-time traffic monitoring, zero-touch provisioning, redundant management ports.
High Availability and Redundancy	Support industry features such as Non-Stop Forwarding (NSF) and graceful restart (GR), redundancy, traffic engineering and hitless software upgrades
Compliance and Certifications:	Compliance to industry standards and certifications with an MTBF (Mean Time Between Failure) of more than 200,000

3. Wireless Access Controller

Requirement	Specifications
General requirements	Equipment shall support enterprise-grade or carrier-class wireless LAN controller (WLC), centralized and distributed deployments (cloud-based, appliance-based, or virtualized), scalable architecture supporting thousands of Access Points (APs) and clients, high availability (HA) with N+1, N+N, or Active-Active redundancy and seamless integration with SDN/NFV and Open APIs (NETCONF, RESTCONF, gRPC, OpenFlow).
Hardware requirements	Equipment shall support hardware appliance (1RU, 2RU, modular chassis) or virtualized deployment (VMware, Hyper-V, KVM, private/public cloud); 50 to 100,000+ APs and 1,000 to 1,000,000 concurrent clients, 1G/10G/25G/40G/100G Ethernet uplink ports, LACP (802.3ad) for link aggregation and Out-of-band (OOB) management port.
Wireless Features	Equipment shall support Wi-Fi 5 (802.11ac), Wi-Fi 6 (802.11ax), and Wi-Fi 6E and beyond, automatic RF optimization (channel selection, power control, load balancing), band steering, airtime fairness, client load balancing, seamless layer 2 and layer 3 roaming, dynamic adjustable transmit power (TPC) and coverage hole detection, multiple SSID and VLAN mapping, pre-SSID traffic shaping, bandwidth control and QoS policies
Security and Authentication	Equipment shall support 802.1X with RADIUS/TACACS+ integration shall support Wi-Fi 5 (802.11ac), Wi-Fi 6 (802.11ax), and Wi-Fi 6E and beyond, automatic RF optimization (channel selection, power control, load balancing), band steering, airtime fairness, client load balancing, seamless layer 2 and layer 3 roaming, dynamic adjustable transmit power (TPC) and coverage hole detection, multiple SSID and VLAN mapping, pre-SSID traffic shaping, bandwidth control and QoS policies, WPA3, WPA2-Enterprise, WPA2-PSK, and Open Authentication, MAC filtering and rogue AP detection/prevention, DDoS protection, wireless IDS/IPS, Guest access with Captive Portal & Social Login and Zero Trust Network Access (ZTNA) & Role-Based Access Control (RBAC).
Network & Traffic Management-	Equipment shall support VLAN and QoS, 802.1Q VLAN tagging, WMM (Wi-Fi Multimedia) support for traffic prioritization, Application-based QoS (Layer 7 DPI), Traffic Optimization, Deep Packet Inspection (DPI) & Application Layer Firewall, and Dynamically adjustable bandwidth limits per SSID, user, or application
Management and Monitoring	Equipment shall support VWeb-based GUI, CLI, SSH, SNMPv2/v3, REST API, cloud-based or on-premises network management, real-time analytics & reporting (RF health, AP status, client connections), Syslog, NetFlow, sFlow support for traffic analysis, Zero-Touch Provisioning (ZTP) & remote firmware upgrades

4. Access Point Indoor

Requirement	Specifications
General requirements	Equipment shall support enterprise-grade Wi-Fi for high-density environments, Dual-band (2.4GHz & 5GHz) or Tri-band (2.4GHz, 5GHz, 6GHz for Wi-Fi 6E) and above, backward compatibility with legacy Wi-Fi standards, 802.3af/at/bt Power over Ethernet (PoE) support for flexible deployments, Standalone, controller-based, and cloud-managed operation and Plenum-rated (UL 2043) for safe ceiling mounting.
Wireless Specifications	Equipment shall support 2x2, 4x4, or 8x8 MIMO and above for increased throughput, OFDMA and MU-MIMO for multi-user efficiency, Channel width support such as 20/40/80MHz (Wi-Fi 5, 802.11ac), 20/40/80/160MHz (Wi-Fi 6, 802.11ax), 6GHz support with 320MHz channels (Wi-Fi 6E/7) and above; transmit power control and dynamic channel selection; aggregate data rate of 3 Gbps or higher, 1024-QAM modulation for high-efficiency transmission, at least 250 concurrent clients per AP; security features namely WPA3, WPA2-Enterprise, WPA2-PSK, 802.1X authentication with RADIUS/TACACS+ integration, MAC address filtering and rogue AP detection, Guest network isolation and captive portal support and integrated firewall and application-based QoS for application-based traffic shaping.
Network and Management Features	Equipment shall support 1x or 2x 1GbE/2.5GbE/10GbE uplink ports for backhaul connectivity, VLAN tagging (802.1Q) and multiple SSID support (min. 8 SSIDs per AP), Zero-Touch Provisioning (ZTP), local and cloud-based management options, SNMPv2/v3, syslog, and real-time analytics, AI-driven RF optimization for interference mitigation, Location-based services (LBS) and Bluetooth Low Energy (BLE) support, Seamless roaming with 802.11k, 802.11v, 802.11r support and IoT readiness (Zigbee, Thread, BLE 5.0).
Compliance and Certifications	Equipment shall conform to industry standards and certifications namely Wi-Fi Alliance Certified (Wi-Fi 6, Wi-Fi 6E, or Wi-Fi 7 ready and above), FCC, CE, RoHS and UL 2043 (for plenum-rated deployments). The equipment shall have ceiling/wall mounting kit included, support PoE (802.3af/at/bt) or DC power input and provide remote and on-site configuration assistance.

5. Access Point Outdoor

Requirement	Specifications
General requirements	Equipment shall support enterprise-grade Wi-Fi for high-density environments, Dual-band (2.4GHz & 5GHz) or Tri-band (2.4GHz, 5GHz, 6GHz for Wi-Fi 6E) and above, backward compatibility with legacy Wi-Fi standards, weatherproof and ruggedized hardware for extreme temperatures and conditions, 802.3af/at/bt Power over Ethernet (PoE) support for flexible deployments and standalone, controller-based, and cloud-managed operation.
Environmental Specifications	Equipment shall support IP67 or IP68-rated enclosure for water and dust resistance, operating temperature of between -40°C to +65°C (-40°F to 149°F), Wind resistance of 165+ mph, lightning and surge protection (EN 61000-4-5 compliance) and UV-resistant housing for long-term durability.
Wireless Specifications	Equipment shall support 2x2, 4x4, or 8x8 MIMO and above for increased throughput, OFDMA and MU-MIMO for multi-user efficiency, Channel width support such as 20/40/80MHz (Wi-Fi 5, 802.11ac), 20/40/80/160MHz (Wi-Fi 6, 802.11ax), 6GHz support with 320MHz channels (Wi-Fi 6E/7) and above; transmit power control and dynamic channel selection; aggregate data rate of 3 Gbps or higher, 1024-QAM modulation for high-efficiency transmission, at least 250 concurrent clients per AP; security features namely WPA3, WPA2-Enterprise, WPA2-PSK encryption, 802.1X authentication with RADIUS/TACACS+ integration, MAC address filtering and rogue AP detection, Guest network isolation and captive portal support and integrated firewall and application-based QoS for application-based traffic shaping.
Network and Management Features	Equipment shall support 1x or 2x 1GbE/2.5GbE/10GbE uplink ports for backhaul connectivity, VLAN tagging (802.1Q) and multiple SSID support (min. 8 SSIDs per AP), Zero-Touch Provisioning (ZTP), local and cloud-based management options, SNMPv2/v3, syslog, and real-time analytics, AI-driven RF optimization for interference mitigation, Seamless roaming with 802.11k, 802.11v, 802.11r support, Integrated GPS for location tracking (optional), Bluetooth Low Energy (BLE) support for IoT applications, external antenna support for directional coverage (optional) and IoT readiness (Zigbee, Thread, Lora WAN support optional).
Compliance and Certifications	Equipment shall conform to industry standards and certifications namely Wi-Fi Alliance Certified (Wi-Fi 6, Wi-Fi 6E, or Wi-Fi 7 ready and above), FCC, CE, RoHS, UL 2043 (for plenum-rated deployments) and WEEE, REACH, EN 300 328, EN 301 893. The equipment supply shall include Pole/wall mounting kit, support for PoE (802.3af/at/bt) or DC power input and enable remote and on-site configuration assistance.

6. Energy Efficiency

Requirement	Specifications
Energy Consumption hotspots	The following are targeted areas in optical networks for energy efficiency: optical transceivers, amplifiers, switching/routing equipment, cooling systems, and passive components (efficient designs can lead to more loss requiring more amplification).
Energy Consumption Improvement Strategies	• Advanced Modulation Format: Use coherent transmission to transmit more data per wavelength reducing the need for additional hardware • Dynamic Power Scaling: Implement adaptive link rates and sleep modes for idle components • Network Architecture Optimization: Deploy Passive Optical Networks (PONs) in access networks to minimize active components and edge computing to reduce long-haul data transmission data. • Energy-Aware Routing: Route traffic through the shortest or least congested paths to minimize energy-intensive amplification • Hollow-Core Fibers: Reduce attenuation by 30% compared to traditional silica fibers, cutting amplify requirements • Renewable Energy Integration: Power remote amplifiers and data centers with solar, wind or hydrogen fuel cells • Silicon photonics: Integrate optical components with silicon chips for lower power consumption and higher integration • AI/ML- Driven Optimization: Use machine learning to predict traffic patterns and dynamically adjust power usage • Software-Defined Networking (SDN): Centralize control to optimize resource allocation and reduce redundant hardware • Quantum-Dot Amplifiers: Emerging technologies with higher efficiencies than EDFAs • Liquid-Cooling: Replace air cooling with direct-to-chip liquid systems for data centers

Annex 2

Public WIFI Inspection and Acceptance Checklist

S/No	Criterion	Inspection Method	Acceptance Threshold	Evidence	Status	Remarks
1.	Approved HLD & LLD	Document verification	Designs approved			
2.	Signed ESIA report and way-leave consents	Document verification	All consents signed and valid			
3.	Risk register & BoQ align with design	Document verification	Registers updated, BoQ signed			
4.	Power-capacity / UPS/grounding plan approved	Document verification	Plan approved			
5.	AP height, azimuth & IP-rated housing correct	Physical inspection	Matches LLD ±0.5 m / ±5			
6.	Indoor cabling in metallic trunking; bends	Physical inspection	Trunking installed; bend radius respected			
7.	PoE switch on dedicated breaker, surge-protected	Physical inspection	Breaker, surge, earthing			
8.	Indoor AP meets Wi-Fi specs	Datasheet check	Spec meets contract			
9.	Outdoor AP IP67/68;	Datasheet check	Spec meets contract			
10	Switch ports & uplinks match contract spec	Datasheet check	24/48 multi-gig, 10 G			
11.	WLAN controller N+1 HA; ZTP enabled	Datasheet check	Controller redundancy confirmed			
12.	Unique SSID(s); captive portal + CIDM active	Config audit	Portal operational			
13.	WPA3 Enterprise enabled; default creds changed	Config audit	Security settings verified			
14.	VLAN / VRF segmentation & client isolation	Config audit	Segmentation active			

S/No	Criterion	Inspection Method	Acceptance Threshold	Evidence	Status	Remarks
15	Content filter & data protection banner live	Config audit	Filter & banner active			
16	Walk-test RSSI ≥ –67 dBm at cell	Field test	Meets signal strength			
17	Throughput ≥ 2 Mbps sustained	Speed test	Meets throughput			
18	Latency <100 Ms • Jitter <30 Ms • Loss <1 %	Ping test	Meets QoS metrics			
19	Seamless roaming between APs (no session drop)	Roaming test	No session drops			
20	Network uptime logs show ≥99 % availability	NMS log review	Meets availability target			
21	OTDR: 1310 nm ≤0.35 dB/km; 1550 nm ≤0.27 dB/km	OTDR test	Meets attenuation spec			
22	End-to-end loss within the design budget	OTDR test	Meets budget			
23	All devices are visible in NMS with telemetry	NMS audit	Devices reporting			
24	Alert thresholds set (link-down, CPU>80 %, uptime<99 %)	NMS config review	Alerts configured			
25	Weekly automated reports scheduled	NMS config review	Reports scheduled			
26	Asset register & PM schedule uploaded	Document check	Register & PM approved			
27	As-built drawings & KMZ routes delivered	Document check	Drawings verified			
28	Configuration backups stored	File check	Backups stored			
29	OTDR & Wi-Fi test reports attached	Document check	Reports complete			
30	Training sign-off sheet (≥4 staff)	Document check	Training verified			
31		Document check	Plan & SLA approved			
32	All defects rectified within 14 days	Inspection	No open defects			
33	Compliance certificate issued	Document check	Certificate issued			

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