



Republic of Zambia

Office of the President
Electronic Government Division

PUBLIC SERVICE INFORMATION COMMUNICATION
TECHNOLOGY STANDARDS

Network Management Standards

First edition 2019 © E-Government Division 2019

Foreword

The Electronic Government (e-Government) Division has been assigned the responsibility of formulating and enforcing Standards in Information and Communication Technology (ICT) across all Ministries, Provinces and Spending Agencies (MPSAs) to facilitate the transition into a Digital Society.

The e-Government Division has therefore issued the Public Service ICT Network Management Standard to ensure adherence and compliance to acceptable Network Management Procedures when implementing ICT networks in the respective MPSAs. These individual ICT networks managed by MPSAs support the rollout of systems and applications in the Public Service that interface with the citizens, businesses and amongst themselves.

The Public Service ICT Network Management Standard will give guidelines on the use and application of Network Management knowledge, processes, skills, tools and techniques which can significantly improve effectiveness and efficiency in achieving public service delivery.

All MPSAs are required to ensure full compliance to this framework for effective and efficient public service delivery.



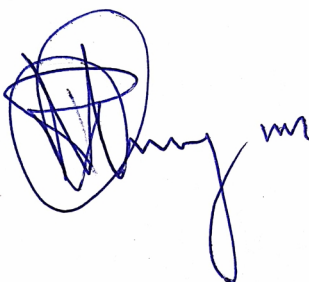
Martine G. Mtonga (Dr)
National Coordinator

SMART ZAMBIA INSTITUTE

Acknowledgement

The development of the Public Service ICT Network Management Standard marks an achievement of a key milestone towards cost effective and efficient implementation of ICT networks in the public service. The Standard will assist Government to ensure a coordinated and collaborative approach to implementation and maintenance of several initiatives under the Government network infrastructure.

I wish to commend the Standards Task Team and various stakeholders as well as the Heads of ICT in Ministries, Provinces and other Spending Agencies (MPSAs) for their unwavering efforts in the development of the Network Management Standard document that will ensure that eGovernment Computer network infrastructure is implemented in an effective and standardized manner.



Percive Chinyama
Director, Standards

SMART ZAMBIA INSTITUTE

Table of Contents

Foreword	i
Acknowledgement.....	ii
Abbreviations	iv
1. INTRODUCTION.....	1
2. NORMATIVE REFERENCES.....	2
3. GNI ARCHITECTURE GENERAL PRINCIPLES.....	3
4. NETWORK MANAGEMENT TEAM	7
5. NETWORK DOCUMENTATION.....	8
6. NETWORK SECURITY	9
7. USER ACCESS.....	10
8. CABLING SECURITY	13
9. POWER SOURCES.....	13
10. MANAGEMENT INFORMATION AND AUDITS.....	14
11. NETWORK STANDARDS AND GUIDELINES	15
12. MINIMUM REQUIREMENTS TO BE ADDED TO THE GWAN	16
13. PROCUREMENT OF INFORMATION AND COMMUNICATION SYSTEMS.....	17
ANNEXES.....	18

Abbreviations

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
DSC/NC	Deputy Secretary to Cabinet/National Coordinator
DTUs	Data Transport Utilities
EIA	Electronic Industry Alliance
FTP	File Transfer Protocol
GRZ	Government of the Republic of Zambia
GNI	Government Network Infrastructure
GWAN	Government Wide Area Network
ICT	Information Communication Technology
IDs	Identification
IDS	Intrusion Detection System
IEE	Institute of Electronics and Engineers
IP/MPLS	Internet Protocol / Multiprotocol Label Switching
IPS	Intrusion Protection Systems
ISO	International Standardisation Organisation
IPV 4/6	Internet Protocol version 4 / 6
ITU	International Telecommunication Union
LAN	Local Area Network

MAN	Metropolitan Area Network
MPSA	Ministry Province or Spending Agency
NOC	Network Operating Center
PABX	Private Automatic Branch Exchange
SNMP	Simple Network Management Protocol
STM	Synchronous Transport Module
SZI	SMART Zambia Institute
VPN	Virtual Private Network
WAN	Wide Area Network

Document Information

File Name	Public Service Network Management Standards Document
Description	Provides compliance requirements for Standards Governing Network Management in Government
Original Authors	ICT Standards Technical Task Team
Creation Date	August, 2018
Last Update	February, 2019
Report Number	1
Version	Version 1.0 (F)
Document Approval	

NAME - SZI Standards

Review Committee	TITLE	Signature	DATE
Dr. Martine G. Mtonga	National Coordinator		
Mr. Percive Chinyama	Director - Standards		

Document Distribution

NAME	TITLE	ORGANISATION
Dr. Martine Mtonga	National Coordinator	SMART Zambia
Mr. Percive Chinyama	Director - Standards	SMART Zambia
Mr. Milner Makuni	Director - EGovernment	SMART Zambia
Stakeholders	Directors and Managers	ZABS, MCT and ZICTA
All Heads of ICT	Heads of ICT	All MPSAs

Document History/Record of Updates

DATE	AUTHOR/S	VERSION	DESCRIPTION
August 2018	ICT Standards Technical Task Team	Issue1.0 (W)	Produced by SZI
October 2018	ICT Standards Technical Task Team	Issue 1.0 (D)	Produced by SZI
February 2019	SZI Management	Issue 1.0 (F)	Produced by SZI

1. INTRODUCTION

This chapter provides standards for design, development, utilisation and management of the Government Network Infrastructure (GNI). It focuses on the standards that support the development and progressive growth of GNI. The main component of the GNI is the Government Wide Area Network (GWAN) which serves as the main Government ICT infrastructure Backbone for linking and inter-connecting MPSAs across the Public Service. The GWAN is intended to:

- a) Provide shared infrastructure services;
- b) Provide a platform for shared services;
- c) Facilitate data, voice and video;
- d) Reduce infrastructure development and management Cost;
- e) Remove/manage duplication;
- f) Enable integration of future technologies;
- g) Enable real time back-up and disaster recovery services;
- h) Provide a comprehensive Network Security solution; and
- i) Facilitate conformity to International Standards.

1.1 Audience

These standards shall be used by Government of the Republic of Zambia Ministries, Provinces and Spending Agencies (MPSAs). The GNI Standards are designed to be inclusive to all users,

bearing in mind the wide range of user needs, circumstances, computer capabilities, technical knowledge and interests.

2. NORMATIVE REFERENCES

All MPSAs connecting to the GNI shall interconnect using the acceptable local and international standards on network management. These include but are not limited to:

2.1 Local Standards

DZS ITU-T G.800	-	Unified functional architecture of Transport Networks
DZS ITU-T G.959.1	-	Optical transport network physical layer interfaces
ZS ITU-T Y.1541	-	Network Performance Objectives for IP-based Services
ZS ITU-T L.1302	-	Assessment of energy efficiency on infrastructure in Data Centers and telecommunication Centers
ZS ITU-T 1210	-	Overview of source-based security troubleshooting mechanisms for internet protocol-based networks

2.2 International

- a) International Organization for Standardization (ISO);
- b) Institute of Electronics and Electrical Engineers (IEEE);
- c) International Telecommunication Union–Telecommunication standardization sector (ITU-T);
- d) Electronic Industries Alliance (EIA);
- e) Telecommunication Industry Association (TIA);
- f) American National Standards Institute (ANSI);
- g) European Telecommunication Standards Institute (ETSI); and
- h) Information Systems Audit and Controls Association (ISACA).

3. GNI ARCHITECTURE GENERAL PRINCIPLES

The planning, design and development of the Government Network Infrastructure (GNI) Architecture shall be guided by the following general principles that support GRZ's strategic business goals and objectives. The GNI shall:

- a) Provide the infrastructure to support GRZ business and administrative processes;
- b) Be operational, reliable and available for essential business processes and mission critical operations;
- c) Provide for scalability and adaptability;
- d) Use industry-proven, mainstream technologies based on open architecture and international network standards;
- e) Be designed with confidentiality and security of data as a high priority;
- f) Allow secure remote accessibility;
- g) Be designed to support converged services while accommodating data, voice and video services and to be "application aware" in the delivery of government services; and
- h) MPSAs shall use standard devices and architecture approved by Office Equipment and Machine Services, Ministry of Works and Supply, Zambia Information and Communications Technology Authority and the e-Government Division.

3.1 GWAN Architecture

For the purpose of these Standards, the GNI Architecture shall include the following components:

- a) **LAN: Local Area Networks** that shall consist of communications systems of multiple interconnected workstations, peripherals, data terminals and other active devices confined to a limited geographic area consisting of a single building or a small cluster of buildings;

- b) **MAN: Metropolitan Area Network shall** consist of communication systems between groups of buildings within a larger geographical area. MAN typically interconnects various communities of interest for information sharing and interoperability using private facilities or public carrier communication facilities;
- c) **WAN: Wide Area Networks** shall consist of communication systems that span a very large geographical area. WANs shall interconnect distributed GRZ facilities and also may function as aggregation mechanisms for various MPSAs with common communication requirements. WANs shall typically use or provide public carrier communication facilities;
- d) There shall be a **Network Operation Center (NOC)** for the GNI that allows for central management and monitoring of all network resources. The NOC shall be providing centralized resources for server management, ICT infrastructure management and monitoring;
- e) GNI Architecture shall use wire-based media, such as copper, and fiber to connect between two or more points, and wireless media such as mobile access points, microwave and satellite; and
- f) GNI Architecture shall also include but will not be limited to Servers and associated storage devices, environment and power control equipment, bandwidth management equipment and telecommunication devices such as Data Terminal Units (DTUs), modems.

3.2 GNI Standards

The following standards shall be used in GNI to interconnect various network resources including technologies, protocols, transport media, topology and naming services. Each technology area shall be classified according to one of the following categories:

- a) **Emerging:** Technologies and products that have the potential to become core in the future. They shall be used only in pilot or test environments, under very controlled restrictions;
- b) **Current Standard In-Use:** These are technologies and products that meet the requirements of the GNI architecture which shall be used in GNI new development projects;

- c) **Legacy:** Existing non-current technologies and products that shall continue to play a substantial role in the architecture for a given timeframe. While not meeting new and future development directions, they remain essential to the existing GNI; and
- d) **Antiquated:** Technologies and products that are currently in use, but no longer have vendor support or are unviable within the GNI Architecture. Their use should gradually be phased out.

The table below describes the standard details that shall be applicable in GNI.

EXAMPLE

Table 1: Standard Details Physical Media		Description
Cabling and plugs		
Classification	Technology Component	
Emerging		
Current Standard in Use	Fibre Single/Multi Mode Optic Fibre, UTP (Cat 6/6a), Structured Cabling System, Coaxial cable	
Legacy	UTP (Cat 5e)	
Antiquated	UTP (Cat 3/4), Telephony	

3.3 Management of GNI

3.3.1 Connectivity Requirements

The GNI shall conform to a set of capabilities and requirements for the functionality applicable to network connections. These include:

- a) To conform to defined open standards and National Network Infrastructure standards;
- b) To provide documentation for user and technical manuals;
- c) To regulate connections at the network level utilizing access control mechanisms and rights;
- d) All connections within GNI shall be based on a standard speed determined by the eGovernment Division;
- e) The GNI shall be built on the IP/MPLS;

- f) The MPSA shall set-up a VPN before getting access to the GNI;
- g) The MPSAs LANs terminations equipment to GNI shall be prescribed by e-Government Division;
- h) The connection technologies supported are, ADSL, ATM, STM, Leased connections, T1/T3, E1/E3, Serial, Frame Relay and Ethernet, Fiber Channel, Fiber Channel over Ethernet; and
- i) MPSAs shall ensure interoperability of all active devices with GNI.

3.4 Connection requests and approvals for GNI

In general, network services provided over the GNI shall be coordinated by the e-Government Division based on MPSAs needs. Such needs shall be requested in writing by the Responsible Officer.

E-Government Division shall issue, certify and revise GNI connectivity requests, standards and compliance mechanisms. At all times, the Government shall retain governance on any connection in operation as follows:

- a) Any connection either established or in the process of being established, shall conform and operate within the established laws, procedures, regulations and standards issued by relevant statutory organisations;
- b) Every MPSA shall be responsible of securing its own network and conform to security policies and international standards that are applicable to any connection and information being transmitted through such connection; and
- c) IP address allocation for the connection link and associated equipment shall be administered by the e-Government Division.

3.5 Suspension and Termination of Connection

The e-Government Division shall reserve the right to suspend the operation or terminate the operation of any network connection or activity on GNI. In the event of suspension of connectivity, re-instatement shall only be possible after authorisation by the National Coordinator e-Government Division. MPSAs shall provide conditionality on reasons for the action (e.g. Non-compliance).

4. NETWORK MANAGEMENT TEAM

The e-Government Division shall have a Network Management Team to be responsible for the GNI. This team shall consist of Network Administrators, System Engineers and Security Experts. Its responsibilities shall include:

- a) Monitoring Network activities;
- b) Implementing Network Security policy;
- c) Performing network control functions to ensure maximum network security;
- d) Receipt and resolution of all network operation escalations for the GNI;
- e) Advice management on emerging Network Technologies and procurement;
- f) Perform Network operations and Administration activities to ensure maximum availability;
- g) Carry out corrective network activities to restore network availability;
- h) Undertake Network Support activities to ensure timely fault repairs and network service restoration; and
- i) Update documentation of network operations procedures.

5. NETWORK DOCUMENTATION

GNI architecture, deployment and enhancements shall be duly documented including documentation on equipment configuration in order to foster proper management, enforce security and plan for growth. This documentation shall be regularly updated and maintained in accordance with change requests.

GNI equipment configurations of the components shall need to be documented for the purposes of maintenance and future planning. GNI vendors shall ensure they provide the original and “as built” documentation. The methods for performing detailed GNI operations shall be defined in the technical resource manuals and training for the GNI. The technical resource manuals shall be classified accordingly and the details on procedures not otherwise defined shall be at the discretion of the e-Government Division.

6. NETWORK SECURITY

The e-Government Division Network Management Team in conjunction with the MPSAs Network Administrators shall oversee the security of GNI and MPSA networks respectively. To maintain the highest level of security surveillance on network performance, the GNI shall be maintained at all times in order to ensure optimized network security and data integrity.

Network Managers shall at all times pay due diligence to configuration and maintenance of access control lists and other security mechanisms on routers, switches, IDS, IPS and firewalls as well as Simple Network Management Protocol (SNMP) security. The managers shall also provide and enforce secure access to devices for both monitoring and management by provisions for role-based management to set access rights for individuals based upon their function and support of authenticated access to the GNI management console.

7. USER ACCESS

Access to the GNI management console shall be protected by user IDs and passwords. The main network administrator shall configure each user and their password and correlate their access to their role. Web access shall be fully SSL, TCL and Kerberos encrypted. Additionally, detailed logging shall be provided in accordance with acceptable security recommendation of all transactions and user driven events on the GNI including:

- a) Individual user access, login and log-off;
- b) Changes to system and monitoring configuration;
- c) Addition or deletion of devices;
- d) Changes to policies, alerts and notifications; and
- e) Access to reporting and other system functions.

7.1 Role Based Management

Along with support for access compliance, the GNI System Administrator shall allow for control of internal access to information and network assets. The Administrator shall directly import user login information from Active Directory and LDAP to speed configuration and provide compliant access control to management tools, information and consoles based upon users' roles and responsibilities. Using roles, there shall be a clear definition, by organizational function, user access to:

- a) Configuration management;
- b) Reporting;
- c) Discovery;
- d) Policies;

- e) Workspaces; and
- f) Management and monitoring of services, servers, applications and devices.

7.2 File Exchange using File Transfer Protocol

With the use of Router Access Control Lists (ACLs), File Exchange using File Transfer Protocol (FTP) shall be restricted to designated ftp servers.

7.3 Electronic Mail Exchange

Official email exchange within the GNI shall be conducted over the network as needed. This shall be enforced and controlled by the MPSA's network/system administrator. All Government communication i.e. Email, Telephone Communication, Video Conferencing, Instant Messaging among others shall be archived legally and accessed for legal services.

7.4 Telnet Access

Telnet access to GNI servers shall be prohibited. Access to other internal Government hosts and devices shall be limited and duly authorized by the relevant authority owning those particular hosts and devices.

7.5 Web Resource Access

Access to internal web resources shall be provided on need basis. Access to the Government's public web resources shall be accomplished through the normal Internet access.

7.6 Protection of Information and Network Resources

The e-Government Division shall be responsible for ensuring that all possible measures have been taken to ensure the integrity and privacy of the government confidential information. MPSAs on their part shall be duly responsible for providing the appropriate security measures

to ensure protection of their private internal network and information. Various measures related to network security shall be followed and this should include:

- a) Bio- Metric Card based login with active directories.
- b) Encryption Method.
- c) Procurement of Systems with adequate security features.

7.7 Physical Security and Entry Controls

The e-Government Division Network Management Team in conjunction with the respective MPSAs Network Administrators shall be responsible for managing Data Centers, training rooms, NOC and Server rooms as well as monitor and review access mechanisms to all ICT facilities. Such shall be achieved by issuing of access cards, passes, biometric facilities and keys among others. ICT facilities supporting critical or sensitive Government services shall be secured.

The security mechanism to be deployed shall include and not be limited to: Use of smooth energy sources, Access control by use of Bio-metrics, Fire safety mechanism put in place and proper environment conditions are adhered to. Critical communications links, computer servers, laboratories, PABX and other priority computing and communications equipment shall be located in physically secure areas.

All single user computer systems that have access to administrative or management information shall be located within an appropriate environment.

Reasonable controls over access and measures to mitigate natural and man-made disasters including fire, flooding, explosion, vandalism and hazards related to electrical power - shall be deployed on such areas. The selection and design of the site shall take into account such risk factors. Consideration shall be given to the following measures:

- a) Hazardous materials shall be stored safely at a safe distance from the site and combustible material such as stationary shall not be stored within the computer room until required;
- b) Fallback equipment and back-up media shall be sited at a safe distance to avoid damage from a disaster at the main site. In particular, Business Continuity Plans and associated equipment shall be stored in a location sufficiently separate to the main location;
- c) Appropriate safety equipment shall be installed in accordance with the Occupational Safety and Health Act;

- d) Emergency evacuation procedures shall be developed with due consideration of the security of the ICT resources; and
- e) Environmental requirements of an equipment room shall be determined by Manufacturer's specification with due diligence and in consultation with certified professionals.

8. CABLING SECURITY

Power or telecommunication cabling carrying data or supporting information and communication technology services shall be adequately protected from interception or damage. All network or communications work shall be conducted in collaboration with the eGovernment Division.

9. POWER SOURCES

Information resources shall be reasonably protected from power failures or other electrical anomalies such as power surges or dips, MPSAs shall use surge protectors and power smoothers. Appropriate testing shall be conducted in accordance with existing Government practices. Backup power sources shall be recommended for equipment supporting critical Government services. These backup power sources shall be regularly tested, and any necessary requirements included as part of any contingency planning processes.

10. MANAGEMENT INFORMATION AND AUDITS

The e-Government Division Network Management Team shall monitor all aspects of connections over the GNI. The use of network monitoring tools shall be employed to automate the auditing tasks needed and complement manual auditing. Auditing shall include the following:

- a) Authentication database showing the specific login entries;
- b) All entity router/network device configurations;
- c) Client equipment where tampering may be reasonably suspected;
- d) Bandwidth management;
- e) Monitoring of access points;
- f) Monitoring dash boards;
- g) Monitoring unauthorized use of network and network facilities; and
- h) GNI to be subjected to external ICT Audit.

The e-Government Division Network Management Team shall investigate any unauthorized changes immediately. All MPSAs connections shall be reviewed on regular basis, by mutual agreement. The e-Government Division Network Management team shall come up with and document routine maintenance processes. The team shall come up with SLAs for the maintenance of network resources with external service providers and ensure that they are adhered to.

11. NETWORK STANDARDS AND GUIDELINES

11.1 Policies and Guidelines

As a general policy associated with this publication, Government entities are required to conform to the standards listed in this document based on their classification and in line with the following recommendations outlined in this chapter:

- a) Ensure that the infrastructure components (network equipment, servers, cabling, etc.) are provided by proven vendors in the market, to protect ICT investments;
- b) Design and build a standard-based network (e.g., MPLS, VPN/IP);
- c) Leverage server virtualisation and hyper-threading technologies when possible to maximize ICT investment utilization;
- d) Build several tiers into the Infrastructure layer design such as separating storage, network equipment, servers and backup solutions, and segmenting those into multiple physical security zones mapped to the design's logical security zones;
- e) Outsource network infrastructure and connectivity to the extent possible, end-to-end, keeping governance and decision making within the Government entity ICT team;
- f) Implement international standards for infrastructure operations (e.g. ISO27001);
- g) Reuse existing infrastructure when possible to reduce costs, and upgrade only when necessary in compliance with the Infrastructure layer standards;
- h) Secure the Government entity infrastructure with end-to-end data encryption (e.g. IP VPN, SSL);
- i) Provide proper training and certification programs of Government entity ICT staff on various infrastructure technologies;
- j) Design, implement and govern a central accountability and responsibility process for infrastructure and security standards and policies;

- k) Integrate the network infrastructure with GNI after complying with its standards and policies; and
- l) Implement a comprehensive backup and recovery plan to ensure that all the Government entity's server and storage contents are secure and recoverable;

12. MINIMUM REQUIREMENTS TO BE ADDED TO THE GWAN

Several prerequisites will need to be satisfied before an MPSA is allowed to join the GWAN. These include a site feasibility study, site readiness activities, and a network security assessment. The e-Government Division will assist in coordinating the following activities:

12.1 Site Feasibility Study

Conducted by a selected team of various skilled individuals identified to include but not be limited to the following:

- a) Satellite, Copper, Microwave, Fiber access to the MPSA; and
- b) Path diversity.

12.2 Site Readiness – ICT Infrastructure room

MPSAs must gather and provide the e-Government Division with the following information not limited to:

- a) Power availability;
- b) Air-conditioning;
- c) Current ICT infrastructure;
- d) Network Access points; and
- e) Cabling.

13. PROCUREMENT OF INFORMATION AND COMMUNICATION SYSTEMS

The objective of these Standards is aimed to assist all MPSAs to know appropriate minimum specifications and standards in procurement and development of Information and Communication Technology systems.

Under the Standards, all MPSAs are expected to obtain technical advice from the eGovernment Division on the configuration of the Information Systems suitable for the purpose intended 15 days prior to issuance of tenders by the MPSAs.

The e-Government Division now has the sole authority to clear all Public Service ICT network infrastructure before they are purchased by MPSAs.

ANNEXES

ANNEX 1 - General Standards

<i>Item</i>	<i>Standard</i>	<i>Classification</i>
1.	All future Government networks must operate using the TCP/IP suite of protocols	Mandatory
2.	All security policies and standards with regards to internal and external connectivity must be addressed in accordance with the Security guidelines provided by the e-Government Division	Mandatory
3.	Delimitalised Zone segmentation should be used for external access to the public network, in conjunction with security standards	Mandatory
4.	All network devices used across the LAN, MAN and WAN infrastructure should be standardized and MUST be subjected to sanitisation process	Mandatory
5.	All WAN-related security services should be a managed service provided by the e-Government Division	Mandatory
6.	Government entities should use a single point of Internet connectivity provided centrally by the e-Government Division, and disconnect all other Internet accesses	Mandatory
7.	The IP network should be designed to handle data, voice, and video traffic	Mandatory
8.	Use of VoIP and IP telephony on the network	Recommended
9.	All network devices used across the LAN, MAN and WAN infrastructure should be able to support IPv6	Recommended

ANNEX 2 - Wide Area Network Standards

<i>Item</i>	<i>Standard</i>	<i>Classification</i>
1.	Use and maintenance of SMTP as the core support protocol for email delivery between Government entities and external parties	Mandatory
2.	Use and maintenance of a DHCP and NAT within MPSAs	Mandatory
3.	Physical data inter connectivity provided by the managed external service provider is based on MPLS technology using IP as the underlying transport	Mandatory
4.	Redundancy must be provided using dual or shared links to allow resilience for all critical components. These links can be physical or wireless links to increase capabilities (operational services and security).	Mandatory
5.	Networks must use TCP/IP industry standard protocols for wired and Mandatory wireless networks, with IP as the only network protocol included in all routers.	
6.	The WAN should be secure, and MPSAs should assess the need to encrypt data over the network	Mandatory
7.	The network must be able to scale with the MPSAs future needs.	Mandatory
8.	The Government must develop and maintain a Government-wide DNS structure.	Recommended
9.	Central remote access services for the entire Government network and connected systems should be available.	Recommended
10.	Integrated service routers should be used to reduce complexity and cost.	Recommended
11.	Transition from IPv4-based networks to IPv6-supported networks should be conducted. Industry vendors are transitioning their products to IPv6, and this transition should be closely monitored.	Recommended

ANNEX 3 - Local Area Network Standards

3.1 Wired Local Area Network

<i>Item</i>	<i>Standard</i>	<i>Classification</i>
1.	Minimum standard switches for each layer are: Workgroup Layer Switch – Should support multiple gigabit Ethernet uplink ports, Ethernet 10/100/1000 ports with IEEE 802.3af Power over Ethernet (PoE) support, high- speed stackable to interconnecting multiple switches, and spanning tree protocol	Mandatory
2.	Core Layer Switch – Should support multi-gigabit service modules (content services, firewall, IP security, VPN, network analysis, and SSL) acceleration, high-performance, high port density fast Ethernet and gigabit Ethernet aggregation, and provide a high level of redundancy within the backplane of switch fabric	Mandatory
3.	QoS - Quality of Service, the switch that analyses the packet contents and applies a traffic class to the switch header. Real-time traffic such as voice must be given highest priority, with data traffic prioritised according to business importance.	Mandatory
4.	Category 6 Copper Cabling Standard	Mandatory
5.	All LAN related security devices, including edge firewalls should be implemented and managed by MPSAs	Mandatory
6.	Cabling infrastructure standards to be followed: ANSI/TIA/EIA-568 series ANSI/TIA/EIA-569 ANSI/TIA/EIA-942	Mandatory
7.	Distribution Layer Switch – Should support high port density fast Ethernet and Gigabit Ethernet aggregation and provide a high level of redundancy, with support for Power over Ethernet (PoE), and spanning tree protocol	Recommended

3.2 Wireless LAN and Wireless Wan Standards

<i>Item</i>	<i>Standard</i>	<i>Classification</i>
1.	802.11i, 802.1X, Wi-Fi Protected Access (WPA), WPA2, advanced encryption standard (AES), and mobile Virtual Private Networks (VPNs) 2.4 and 5 GHz integrated diversity.	Mandatory
2.	Recommended minimum standards for Wireless Access Points are the IEEE 802.11x series of standards address WLAN standards. Four of the 802.11x standards address the physical layer, and current standards are 802.11a, 802.11b (Wi-Fi), 802.11g, and 802.11n offering 54Mbps, 11Mbps, 54Mbps, and 248Mbps respectively.	Recommended
3.	Directional antennas or 2.4 and 5 GHz dual-diversity RP- TNC connectors for external antenna with support for inline power.	Recommended
4.	WWAN transport technologies: WIMAX, UMTS, GPRS, CDMA2000, GSM, CDPD, HSDPA or 3G, LTE and 802.16	Recommended

ANNEX 4 - Voice Network

<i>Item</i>	<i>Standard</i>	<i>Classification</i>
1.	Use of voice-enabled routers for WAN connectivity. However, devices connected to the Internet may have voice restrictions. It is recommended that this be discussed with the service provider and be disabled if required.	Recommended
2.	Skinny Client Control Protocol (SCCP). An H.323 proxy can be used to communicate with the skinny client using the SCCP. In such a case the telephone is a skinny client over IP. The skinny client (i.e., an Ethernet phone) uses TCP/ IP to transmit and receive calls and RTP/UDP/IP to/from a skinny client or H.323 terminal for audio.	Recommended
3.	Use of duly licensed telecommunications network operators and service providers for local PSTN connectivity for external telephony, with define SLAs.	Mandatory
4.	The H.323 standard provides a foundation for audio, video, and data communications across IP - based networks, including the Internet. H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over LANs. Therefore, the H.323 standards are important building blocks for a broad new range of collaborative, LAN-based applications for multimedia communications.	Recommended
5.	If voice-enabled routing is designed within the architecture, voice-enabled switching technology must be used as a design principle.	Recommended

