Republic of Kenya

PRESIDENCY AND CABINET AFFAIRS OFFICE

OFFICE OF THE PRESIDENT

ICT STANDARDS AND GUIDELINES

Developed by the Directorate of e-Government

Version 0.1

Public services everywhere, all the time!

March, 2011

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ADSL	-	Asymmetrical Digital Subscriber Line
ATM	-	Asynchronous Transfer Mode
COTS	-	Commercial-off-the-Shelf
CPU	-	Central Processing Unit
CSS	-	Cascading Style Sheets
DeG	-	Directorate of e-Government
FAQs	-	Frequently Asked Questions
FTP	-	File Transfer Protocol
GNI	-	Government Network Infrastructure
GoK	-	Government of Kenya
GWI	-	Government WAN Infrastructure
HTML	-	Hyper Text Markup Language
HTTP	-	Hyper Text Transport Protocol
ICT	-	Information Communication Technology
ICTSP	-	Information Communication Technology Security Policy
IDS	-	Intrusion Detection System
IEC	-	International Electro-technical commission
I/O	-	Input/output
IP	-	Internet Protocol
IPv4	-	Internet Protocol Version 4
IPv6	-	Internet Protocol Version 6
IPS	-	Intrusion Prevention System
ISO	-	International Standards Organization
ISP	-	Internet Service Provider
IT	-	Information Technology
KCA	-	Kenya Communication Amendment
KNA	-	Kenya News Agency
LAN	-	Local Area Network
MAN	-	Metropolitan Area Network
MB	-	Megabyte
MDA	-	Ministry/Department/Agency
MPLS	-	Multiprotocol Label Switching
NOC	-	Network Operation Center
OPC	-	Office of Public Communications
OSI	-	Open System Interconnect
PC	-	Personal Computer
PDF	-	Portable Document Format
PSCK	-	Public Service Commission
PTAD	-	Project Team for Application Development
RAD	-	Rapid Application Development
RFC	-	Request for Comments
SAS	-	Statistical Analysis Software
SDLC	-	Software Development Lifecycle
SNMP	-	Simple Network Management Protocol
SPSS	-	Statistical Package for the Social Sciences

SQL	-	Structured Query Language
TCP	-	Transmission Control Protocol
TFTP	-	Trivial File Transfer Protocol
URL	-	Uniform Resource Locator
VOIP	-	Voice Over Internet Protocol
VPN	-	Virtual Private Network
W3C	-	World Wide Web Consortium
WAI	-	Web Accessibility Initiative
WAN	-	Wide Area Network
WCAG	-	Web Content Accessibility Guidelines
WWW	-	World Wide Web
XHTML	-	Extensible Hyper Text Markup Language

LIST OF TABLES

FOREWORD

The Government of Kenya recognizes the value of using ICTs and the Internet as a means enhancing communication and exchange information, delivering services and interacting better with citizens and consumers. As Government increasingly uses ICTs and the Internet it is becoming more important that a common approach based on recognized best practices is taken. The Government therefore recognizes the need for a consistent approach to the use of ICTs and the Internet and thus the formulation of this ICT Standards Document to provide citizens and all its customers with high quality, consistent, accessible and useable online and offline services.

The e-Government Strategy shall guide the development and use ICTs and the Internet. The Government has a responsibility to all Kenyans and others who enquire and seek for its services and there's therefore a need to minimize the effects of the 'digital divide' by ensuring that Kenyans have equal access to all services and information. This means ensuring that information is available to all people, regardless of disability, bandwidth, location, reduced mobility and age or language barriers.

The principles set out in this document shall be applied across Government in the usage of ICTs and the Internet and by those involved in offering a service or information to the public using the same, including senior management, ICT Officers, public relations officers, information officers, professionals and advisers supporting all-manner of service delivery and those tendering for or providing ICTs and Internet services.

This policy document provides guidance and a consistent approach across Government in establishing, acquiring and maintaining current and future websites, networks, software applications as well as hardware. Its development is based on internationally recognized best practice principles and was done in consultation with a vast array of subject experts and interest groups, with input from all Government MDAs. It shall be used in accordance with the e-Government Strategy and be reviewed and updated regularly thereof.

AMB. FRANCIS K. MUTHAURA, EGH
PERMANENT SECRETARY/SECRETARY TO THE CABINET AND
HEAD OF THE PUBLIC SERVICE

ACKNOWLEDGMENTS

The Directorate of e-Government wishes to extend its sincere appreciation to the Permanent Secretary, Secretary to the Cabinet and Head of Public Service, Mr. Amb. Francis Muthaura, EGH, and the Principal Administrative Secretary Mr. Sam Mwale for their continued support and commitment to leveraging e-Government in public service delivery, reform and transformation. Their dedication in overseeing the development of these standards to facilitate coherence and consistence across public service in delivering e-Government cannot be gainsaid.

The Directorate would like to acknowledge the efforts of Heads of ICT units in ministries/departments whose contributions have made the preparation of these standards possible. The Directorate also wishes to thank the Standards team for working tirelessly in developing these standards. Special thanks go to Francis Mwaura, Mary Kerema, Patrick Njoroge, Bernard Ajwang, John Njoroge, Fridah Miriti, Violet Murwa, Priscilla Maina, Prudence Kirimi and Arpharxard Kioko for their steadfast commitment and dedication to the team activities and their devotion during the preparation of this document.

Many thanks go to the administration, accounts and procurement units of the Cabinet for the unwavering and steadfast support in facilitating sourcing for various goods, materials and services that the team so deservedly required in putting together these standards. Lastly, the Directorate extends sincere gratitude and appreciation to all those who assisted in various ways to make the compilation of standards a success.

DR. KATHERINE GETAO,
ICT SECRETARY,
DIRECTORATE OF E-GOVERNMENT
APRIL, 2011

CHAPTER 1

INTRODUCTION

This ICT Standards document has four (4) main sections:

1. Web Development and Management
2. Network Infrastructure Management Guidelines
3. Software Acquisition Guidelines
4. ICT Equipment Management Guidelines

Background

This ICT Standards document is designed to guide government Ministries, Departments, Agencies (MDAs) in adoption of common standards in order to promote good practices in the Government-wide use of ICTs and the Internet.

This document presumes the reader has some familiarity with basic ICTs and Internet terminology, development and design. It summarizes key aspects of ICT and Internet issues and is intended to act as a ready reference guide.

Purpose

The purpose of these standards is to give guidelines that will assist to promote excellence in public sector management through use ICTs and the Internet. This document should be viewed as an information resource containing standards and best practice guidelines for government MDAs to refer to when using ICTs and the Internet.

These guidelines address common policy issues and practical challenges that MDAs face when using ICTs and the Internet. Some shall assist MDAs to overcome implementation problems, while others provide guidance about the approach to adopt where no obvious choice currently exists. The use of these guidelines shall help to ensure that the use ICTs and the Internet across government in the delivery of its services is done to a consistently high standard. This shall lead to increased confidence and rapid uptake in the use ICTs and the Internet within Government as well as increased customer satisfaction in government services enhanced by both diversity of deliver channels as well as prudent use the same.

Most traffic on the internet uses Internet Protocol Version 4 (IPv4) addresses on all the devices, namely computers, servers, routers, switches and access points. IPv4 was designed to use 32-bit addressing and can handle approximately 4.3 billion addresses. To date 90% of IPv4 addresses has been allocated and the remaining 10% will be exhausted by end of 2012. Internet Protocol Version 6 (IPv6) is the next generation internet protocol and was created to solve the overcrowding problem in the IPv4 address space. IPv6 uses a 128-bit address and provides 2**^128** possible IP addresses. In recognition of the impending exhaustion IPv4 addresses, a global migration to IPv6 is underway. The Directorate of e-Government therefore recommends:

- Procurement of IPv6 capable products in Government;
- That Internet Service Providers (ISPs) to government shall make available IPv6 services native in order to support the large number of mobile devices;
- Internet content and applications shall be reachable using both IPv4 and IPv6 (Dual-Stack environment);
- The industry should be made aware of the impending migration in order that they are able to offer support to equipment and software;
- Establishment of a Government Centre of Excellence to create IPv6 awareness by training, educating, advicing and sharing of best practices.
- Ministries to review current programmes and upgrade to ensure IPv6 compliance.

1.1 Web Development and Management

The purpose of the Internet is to provide users with access to information and services. For government, it is a method of providing information and services to consumers in an efficient and effective manner. If used well, the Internet also provides government with a means of providing consumers with an increased range and quality of service.

The huge opportunity provided by the growing Information Age society and the demand for electronic services delivery creates the need to have Government Websites that provide all Kenyans with access into the operations and services of their Government, in line with the e-Government Strategy. Over time these Websites should be able to allow consumers to find the information and advice they seek, transact services in a safe and convenient electronic environment, and participate in policy creation and other democratic processes of the government.

Government Websites should provide convenient channels that assist consumers identify what services they require, before guiding them through the process to obtain these services. Progressively they should bring about an end to the need for travel to physical Government offices to transact business. This shall, with time, reduce the compliance burden on each and every Kenyan.

However, to be successful in providing quality online services, government agencies must ensure that the same quality of service principles associated with the delivery of offline services, are applied to online services. This incorporates all aspects of web delivery, from the identification of the objectives for websites and the development of business cases, through to their management and maintenance.

Use of open standard based tools and technologies for the development of websites as well as content is very important to interoperability and accessibility of websites. The web guidelines in this document adhere to the Web Content Accessibility Guidelines (WCAG) of the World Wide Web Consortium (W3C). W3C is an international body working towards defining standards in web technologies and formats for publishing contents on the web.

1.2 Network Infrastructure Management

The Government Network Infrastructure (GNI) 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. The GNI architecture is primarily constructed around an Internet Protocol based network. The network is composed of industry standard equipment, which also provides flexibility and a large variety of management and diagnostic tools.

The GNI shall be protected from other data networks in order to enforce its security and functionality. If there is a connection to another data network, it shall be through an appropriately designed and maintained firewall. All the components of the network shall be owned by the Government of Kenya (GoK).

The GNI backbone is structured on an integrated network; any infrastructure hardware and software upgrades or changes that may impact the system network shall need reasonable discussion and subsequent approval by the Directorate of e-Government (DeG). All maintenance work being scheduled that may affect the GNI performance shall be preceded by reasonable and appropriate notification to all MDAs.

The equipment configurations of the components of the network shall be documented for the purpose of maintenance and future planning. The methods for performing detailed network operations shall be defined in the technical resource manuals and training for the GNI. The details on procedures not otherwise defined shall be at the discretion of DeG. There shall be a Network Management Team responsible for the maintenance of GNI network sites and equipment, while MDA Network Administrators shall be responsible for managing the data attributes that they are individually responsible for.

1.3 Software Guidelines

Application development refers to a software development process used by an application developer to build application systems. This process is commonly known as the Software Development Lifecycle (SDLC) methodology and encompasses all activities to develop an application system and put it into production, including requirements gathering, analysis, design, construction, implementation, and maintenance stages. SDLC methodologies include waterfall, iterative, rapid, spiral, RAD.

Application development methodologies are generally developed to guide software application development processes. The key application development methodologies to be used within the GoK are Waterfall and Iterative. Generally, the critical objectives, activities and deliverables of each of these methodologies remain the same. This document specifies the application development standard that is applicable for Waterfall and Iterative methodologies. Government agencies and application developers will use this standard to help guide project teams to develop applications in a consistent, standard and predictable manner.

Effective application development processes are critical to the success of IT projects. Project Teams for Applications Development (PTAD) must select and follow one of the many applications development processes that can be categorized as Waterfall or Iterative. This standard clearly defines expected application development activities, measures and deliverables for each phase of the development methodology used, to help in ensuring that the necessary standards are maintained through the entire life of the project. Projects must select one application development methodology and use it for the duration of the entire project.

1.4 ICT Equipment Management Guidelines

In an ever-changing and dynamic world, the advent and adoption of ICT across the globe has continued change the way of doing business and significantly raised expectations of the new digital and inter-connected economies. The role of ICT in advancing the growth of national economies through enhanced efficiency and productivity, and expanded market reach is both undisputed and irreversible.

The Government of Kenya therefore sees the need to place adequate and strategic attention to these new opportunities provided by ICT by ensuring that they are not purely limited and accessible only by the large corporations within national economies, but also to local public sector organizations. Successful use and management of ICT will continue to improve as well as enable Government to serve all its customers better.

CHAPTER 2

WEB DEVELOPMENT AND MANAGEMENT

2.1 Government Information Online

The vast majority of people use the Internet to access information. The Internet is becoming a preferred means of accessing government information and services. Therefore, a crucial element of an effective web presence is quality and relevance of information. Government MDAs shall develop websites that contain informative and up-to-date content that is well-written, caters for the needs of a wide range of audiences and is easily accessible. They must therefore ensure that:

- Information provided on website meets the needs of consumers
- Information provided is current
- There is a consistent approach across websites
- At least a minimum set of information is provided

Information presented on a government website must be consistent with government policies to avoid the possibility of damage to both the government and consumers if information is incorrect or inappropriate.

There shall be a similar structure applied across government websites to achieve consistency, which is important in helping consumers to access government information more effectively online. Further, in order that government information is visible to everyone all over the world, all Government information online shall run on both IPv4 and IPv6 platforms.

2.1.1 Recommended Level of Information Provision

It is recommended, as best practice, that government MDAs include publications that are available to the public through other forms of media (such as hardcopy or audio) on their websites. The same shall be captured linked in the online library. Where this is not practicable – due to, for instance., high costs, limited benefits, low demand, publication complexity - information on how to obtain a copy in its original form should be posted on the website. Any decision not to publish in electronic form rests with an appropriate senior executive or delegate.

2.1.2 Home Pages

There are certain necessary information elements which are important in a government website. It is therefore required that home pages shall include but not limited to:

- Website Banner
    - Government of Kenya Coat of Arms
    - MDA Name

    - MDA Logo, where applicable
    - Colors of the National flag
- About the MDA, and links to:
    - Organizational set-up
    - Role and Functions (Mission, Vision, Mandate)
    - Major projects and Schemes
    - Public Services
    - Publications e.g. Annual reports, strategy documents, portfolio budget statements
    - Customer Service Charter
    - Government Tenders
    - Press Releases / Announcements
    - Associated Organizations (Related Links)
    - Messages/Speeches from the Minister / Permanent Secretary
    - Contact Addresses / Telephone Number / Email of the Senior Officers and Important Functionaries of the Ministry/Department
    - A feedback/comment page and FAQS
- Search Engine
- Site Map
- Date, time, currency, telephone details
- Physical location information

The manager of each government website must continuously endeavor to determine the kind of information that would benefit the website's audience so as to provide it appropriately. Individual pages for the respective websites should have a consistent look and feel. It is recommended to include in the footer details at the base of each page i.e. the date created and last updated date, where technically possible, and a link to the "Contact Us", privacy statement and disclaimer pages.

2.1.3 Enquiries and Feedback

Government MDAs are required to provide full contact details, including physical service locations, fax and telephone numbers, and mailing addresses. Email addresses shall also be provided, in particular, for the entity responsible for maintaining the website for the purpose of reporting fault. A general enquiry email address for the MDA shall be established so as to protect the individual name and person, which consumers can contact in relation to the MDA service offerings.

Contact email addresses shall be role–based, rather than person–based. This shall allow emails to be distributed to one or more individuals within the MDA and eliminate website maintenance when personnel changes occur within a MDA. Web forms shall be provided, where users can enter their message, submit it and the message gets emailed to the delegated recipient. A further refinement is to email the sender a copy of the message for their records. There shall be a link for consumers to log complaints and a proper feedback mechanism put in place, all the complaints shall be responded to within 24 hours and proper records maintained.

It is worthwhile to note that email addresses listed on a government website that include a readable email address can open the delivery of spam, viruses and other security issues. Therefore an MDA shall give consideration to the number of addresses provided.

.1.4 Legislative and Sectoral Information

Policy documents, legislative and sectoral information related to the MDA shall be provided on their website. This information shall not be duplicated on any other MDA websites, instead links shall be provided to relevant resources at the various source websites. These include, but not limited to:

- The Constitution of Kenya
- Bills, Acts and Treaties
- Subordinate legislation and legislative status information
- Sectoral policy documents
- Circulars, Policy Documents, Schemes of Service, Publications, Reports

2.1.5 Forms

There are several types of forms that can be use to present and collect information from users; Interactive forms, e-forms and downloadable forms.

For interactive forms, appropriate security precautions shall be put in place to safeguard user information during transmission and storage. MDAs shall also ensure that user input errors are minimized by helping users identify, avoid and correct mistakes.

MDAs shall ensure that e-forms and downloadable forms are in compatible formats and where special software is required, a link to download it must be provided. For these types of forms, pdf format is recommended.

Government MDAs shall continuously endeavor to provide online interactive forms, and where not possible, a downloadable format shall be made available. All open forms like registration/feedback forms shall have CAPTCHA implementation.

2.1.6 Types of Information not permitted

Government websites shall not post information that does not promote the MDA of Government policy. In addition, the following content shall not be permitted:

- Commercial banner advertisements
- Personal information
- Politically partisan content

Government websites can however acknowledge sponsors and partners at a section on their website but this decision rests with the appropriate senior executive within the MDA, provided it is consistent with government policy.

Banners that promote and link to other government MDAs are permissible, provided that no fees are charged in placing such banners.

2.2 Web Design and Content Management

Government websites shall be developed in a precise, concise and objective manner. To ensure content is suitable for the web, three main principles shall be considered:

- Be succinct; highlight only key aspects and provide links to the original content.
- Write for scannability; users should not be required to read long continuous blocks of text. Use links to split up long text into multiple pages.
- Use plain English; hyped promotional writing, departmental jargon or bureaucratic language should be avoided.

Government websites shall be developed using a Content Management System (CMS). The CMS shall guide design and structure of the website. The design shall have a consistent layout to aid in navigation and incorporate a help facility. MDAs shall use a pre-designed website template to establish a visual identity and apply it throughout the website. This template shall be provided to MDAs by DeG following relevant consultations.

2.2.1 Design Guidelines and Website Structure

2.2.1.1 Audience

Government websites shall aim to be inclusive to all users, bearing in mind the wide range of consumers' circumstances, computer and other access devices capability, technical knowledge and interests. The website structure shall be user-centric.

In order to ensure accessibility for all citizens, government websites shall respond to consumer requirements. In planning websites an MDA shall carry out market research and consultation with the target audiences and the general public. This shall be done periodically as part of a quality review process.

MDAs shall ensure that web content is more accessible to people with disabilities including visual, auditory, physical, speech, cognitive, language, learning, and neurological disabilities.

2.2.1.2 Hierarchy and Structure

Government MDAs shall establish a clear web content management structure. Website structure entails organizing the website's content, information flow and category or subject hierarchy in such a way that users can logically move through the website with ease, track their progress and determine their location within the website on any web page by use of a site map.

Taking into account consumer expectations and the functionality to be delivered, MDAs shall provide either:

- A hierarchical structure, where pages are grouped according to a number of attributes or categories. This is the most effective method for organizing large volumes of information.
- A linear structure, where pages are presented in a logical sequence. This approach is best suited for search results that present information alphabetically or according to ranking.
- Or a combination of the two as the circumstances may demand.

2.2.1.3 Page Layout

Government MDAs shall endeavor to design pages that are informative, inviting, concise and easy-to-read and organize content using headings. They shall provide enough information for visitors to recognize what is being offered, explore further and easily navigate the website. The design should minimize clutter in the form of distracting animations, splash pages, unnecessary graphic elements and blinking or scrolling text.

2.2.1.4 Navigation

Government websites shall use navigational links and labels that are easily recognized and widely accepted such as Home, About Us, What's New, Media Releases, Publications, Search, Contact Us, Useful Links, Site Map, Feedback and Help. To provide consistent navigational links, MDAs shall ensure:

- The navigation system shall be insightful to help consumers easily locate information or services
- Links to the home page and the search facility shall be provided on every page.
- 'Breadcrumbs' are provided at the top of each web page
- Provide ways to help users navigate, find content, and determine where they are by ensuring tab order reflects navigational sequence.

2.2.2 Quality of Web Content

MDAs shall ensure that the content created for the website is of high quality, accurate, current and meets the needs of the users and the requirements of the government. Within these recommended parameters, an MDA shall adhere to the prevailing guidelines provided.

2.2.3 Content Management

Content is key to every website. Government MDAs shall therefore continuously endeavor to create web content that reflect relevancy and currency. Presentation of content shall seek to limit each page to one concept as well as provide information based on the six principles of journalism: who, what, when, where, why and how and ensure that the content is written in a style suitable for the web.

2.2.3.1 Content Characteristics

MDAs shall ensure that web content has the following characteristics:

- Presentability – Consider the characteristics of created documents and how to best present them. Downloadable versions are recommended for lengthy documents. For PDF files, provide a link to the latest Document Reader.
- Authenticity – Each document included shall contain the following, but not limited to:
    - Status of the document, where applicable
    - Author and date
    - Version and location of the original publication
    - Contact details and feedback mechanisms
- Adaptability; Create content that can be presented in different ways without losing information or structure
- Functionality; Web components shall work correctly and quickly
- Usability; Website shall be simple and well organized
- Relevancy; Web content shall be meaningful to the target audiences
- Distinguishability; Make content easier for users to see and hear including separating foreground from background
- Operability – All functionality of the content should be operable through a key board interface without requiring further user intervention
- Readability; Make content readable and understandable
- Well-written; good grammar and spelling
- Appearance; Shall be appealing to the target audiences
- Timely; up to date content
- Compatibility; Content shall be accessible through the various media, end user devices and across different browser platforms
- Robustness; Content must be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies.

2.2.3.2 File Formats

To ensure consistency, compatibility and fast-loading pages, it is recommended that the following file formats be used.

- Document – All downloadable documents shall be in PDF format
- Audio – Audio files shall be in .mp3 format
- Video - Video files shall be in .mp4, .flv formats
- Graphic – Image files shall be in .jpg, .gif, .png formats

MDAs shall also provide text alternatives for graphics, video and audio clips as well as ensure that all the content takes care of the people with visual and hearing disabilities. Use of sign language interpreters for audio files and provision of extended audio description for videos is recommended whenever possible.

While it is important to include multimedia content including text, audio, still images, animations, video and interactive content forms, MDAs shall ensure that such content does not distract from the main message, irritate users or lead to unacceptable download times.

2.2.3.3 Writing Style

While writing for the web, MDAs shall endeavor to:

- Make the text easy and quick to read
- Use highlighted keywords
- Use meaningful/descriptive titles, link texts and subheadings
- Use bulleted lists
- Use plain English - Avoid acronyms, jargon, and complex words.
- Ensure content is free of material that could be generally considered offensive.
- Use correct punctuation.
- Ensure correct spelling is used.
- Check the context in which the writing is done to ensure correct wording is used.

2.2.3.4 Text Formatting

Web content shall be presented in suitable font sizes and styles. When formatting text, MDAs shall endeavor to:

- Use font size 12 for legibility and readability of text. Users should be presented with an option of font size adjustments.
- Maximize readability by making text left–justified.
- Use the bold font style, for highlights or emphasis.
- Avoid underlining text. It can be mistaken for a hyperlink.
- Avoid using colour text. This may be difficult to read or may present difficulty for the colour blind.
- Italicize references to published documents such as reports, Acts.
- Ensure headings are in sentence case format, with the initial letter of the first word capitalized, with all remaining letters, except for proper nouns, in lower case.
- Caption acronyms wherever they are referred and a list of acronyms and glossary shall be provided.

2.2.3.5 Web Development

During web development, MDA websites shall validate to following technologies for published grammars:

- HTML 4.01
- XHTML 1.0
- XML 1.0

MDA websites shall endeavor to use Cascading Style Sheets (CSS) as much as possible to control layouts/styles. Server side scripting languages should be preferred over client side since client side scripting may face issues of browser compatibility, scripts being turned off by browsers, security, among others. Websites should be validated and tested with both automatic tools and human review.

2.3 Website Management

Government MDAs shall ensure that delivering information and services on the Internet is managed with the same level of quality and commitment as that employed when delivering information and services using conventional methods. The management of online services in a government MDA requires the establishment of a Website management committee, with representation from all key departments including a Webmaster. The committee shall be required to develop and oversee implementation of a Website management strategy.

The Directorate of e-Government shall ensure conformity to the laid down guidelines by constituting a web management unit.

2.3.1 Website Management Committee

The ownership of the MDA website and the quality, relevance and currency of its content shall be vested in the Accounting/Authorized Officer. The Website Management Committee shall constitute of:

- Accounting/Authorized Officer - Chair
- Head of ICT Unit – Secretary
- Head of Communications
- A representative from key directorates/departments/units
- Public Relations Officer (PRO)
- Legal Officer
- Webmaster

The Website Management Committee shall be mandated to:

- Ensure that websites are developed and maintained according to the set standards, policies and guidelines, and that the MDA informs DeG accordingly
- Ensure that the website is positioned as a major communication and service delivery tool
- Collate and validate web content
- Identify and recommend the resources and support requirements to ensure effective website performance
- Ensure that online systems are developed and integrated so as to maximize access, effectiveness and ease of use
- Undertake periodic web content reviews to ensure the integrity, reliability, accuracy, currency, consistency and completeness of the content.

- Formulate a web security plan/policy to address various security issues
- Develop strategies:
  - To ensure the web content is maintained and presented in a manner that supports communication and service delivery objectives
  - To ensure the web content and enquiry solutions for customer relationship management are built on sound business processes and workflow practices
  - For promoting the website
  - For content lifecycle and archival management
- Prepare and submit quarterly reports on the status of implementation of the MDA website management strategy to the Directorate of e-Government
- Review cabinet/ministerial correspondence for possible improvements that may be undertaken
- Monitor reported problems and consumer queries over a period of time, ensure appropriate corrective action is taken and that user feedback is responded within stipulated SLA.
- Undertake consumer surveys, refine the service objectives of the website in light of results from the surveys, keep access statistics and realigning the website information and services as appropriate.
- Give approval for decommissioning of website(s)

2.3.2 Website Management Strategy

The website management strategy shall include activities and timelines, as well as the development and regular review of all plans associated with the website, including:

- Objective of the strategy
- Online services plan
- Financial plan
- Information management plan to include content maintenance, timely updating and decommissioning of websites
- Electronic record management and archiving plan
- Information Education and Communication (IEC) plan
- Customer relationship management plan
- Monitoring and Evaluation plan
- Website security plan
- Risk management plan

2.3.3 The Webmaster

MDAs shall appoint a webmaster who shall update web content on a regular basis with the approval of the website management committee. Consideration shall be given to new features being promoted to consumers and closely monitor their responses. Webmaster duties shall also include but not limited to:

- Designing and publishing web pages
- Installation of web software(s)
- Website configuration and bug fixes
- Website traffic monitoring
- Website maintenance
- Web security enforcement
- Analyzing Server Log Files
- Produce a monthly report on Web Statistics, Analytics, Traffic Stats, etc
- Participate in the Government Webmasters Forum

2.3.4 Consumer Feedback

MDAs shall use consumer feedback as a primary indicator of the success of the website. Consumer feedback can help in determining website relevance, usefulness, currency of information and quality. All problems and consumer queries shall be attended to in a timely and professional manner. Officers shall be assigned to:

- Review reported compliments, comments, problems and queries
- Forward them to the appropriate office in the MDA for action
- Monitor timeliness of corrective action
- Respond to the consumer within defined timeframes

2.3.5 Regular Research

MDAs shall conduct consumer surveys on a regular basis to enable continuous improvement of the website. The research shall seek to determine the:

- Usefulness of information resources and services offered on the website
- New information resources and services to be provided
- Identification of web pages and online services that are slow to load
- Ease of locating required information and services
- Accessibility and usability
- Suggested improvements
- Consumer statistics

2.3.6 Documentation

MDAs shall produce and maintain documentation of the development processes, administration and maintenance of the website including internet applications and databases for continuity.

2.3.7 Decommissioning Websites

Government websites shall be regularly reviewed to ensure that they are relevant and up-to-date. A websites shall be retired where: it:

- Does not serve a specific function or purpose of government
- Has been rendered irrelevant due to re-organization of government
- Was developed for a particular project or strategy that is no longer relevant or current
- Was launched as part of a government-sponsored campaign that has since come to an end
- Is non-essential and website traffic statistics, where available, shows that the website is not being utilized.

When decommissioning websites, consideration shall be given to archiving the content as appropriate.

2.3.8 Web Management Unit

The Directorate of e-Government (DeG) shall establish a Web Management Unit, consisting of Webmasters, Information Experts, Security Experts, Application Developers and Database Administrators. This Unit shall ensure that all Government websites adhere to set web standards and guidelines. It shall also:

- Develop the Government Portal Strategy
- Design, develop, manage and document the Government Portal
- Liaise with MDAs to produce and improve content of the Portal
- Design and develop a common website template for Government websites
- Ensure that all Government websites are developed on a common and secure CMS platform
- Support MDAs in developing their websites upon request
- Host government websites and manage the web server
- Register and maintain web domains
- Conduct quality control of the government websites, and as necessary recommend to MDAs the use of current web technologies to adapt to changing requirements, and create awareness
- Identify and recommend relevant web training for webmasters, ICT officers and other Government officers
- Do periodic accessibility audits for all government websites and produce audit reports accordingly
- Develop and regularly review web guidelines, reports and plans related to government websites
- Identify online systems and projects for benchmarking, locally and internationally
- Provide support to webmasters in MDAs
- Coordinate a Government Webmasters Forum

2.4 Government Portal

The Government Portal shall provide a single gateway to the Government of Kenya. The portal shall be in English with translation in Kiswahili. The primary users of the portal will be the various general publics including the citizen, private sector and non-governmental consumers, public sector consumers, the international community, researchers among others. The portal shall endeavour to provide the ideal mechanism for consumers to access government information and services. MDAs that meet the access platform guidelines shall be linked to the Government portal.

There shall be a citizen-centric Government portal strategy which shall ensure continuous improvement of the portal to facilitate the achievement of the e-Government vision. The strategy shall define the objectives of the portal and provide for its continuous development as well as a benchmark for measuring performance, with the view to optimizing the delivery of online services to the public. The portal shall focus on government news online, information and various public services such as online recruitment and government library.

2.5 Access Platforms

MDAs shall endeavor to ensure that all websites can be displayed on all standard browsers. Taking cognizance of the ubiquity of the mobile devices, MDAs shall endeavor to use access platforms far beyond the traditional web browser in order to bring services closer to the majority particularly in the rural areas. Web services shall therefore be designed for delivery through various access devices mobile telephones, PDAs, IPADs, and digital TVs among others. Consumer feedback shall be ensured where these platforms are used, and where transactions are not successful mechanisms to reverse the transaction shall be available. All access platforms shall be adequately secured taking into consideration issues of authentication and repudiation.

2.6 Government 2.0 and Social Media

MDAs shall endeavor to embrace the use of Web 2.0/Government 2.0 standards in delivering content to individual users. Such applications include wikis, blogs, customized individual and team web pages, portlets, among others. This technology whose aim is to customize the web service experience to the target user shall at all times be upheld. MDAs shall however ensure that they appropriate caution to mitigate against the inherent risks is observed.

The existence of social media presents an opportunity to network for MDAs. For example MDA pages on Facebook or Twitter. MDAs must have authority from the Presidency and Cabinet Affairs Office (PCAO) before such technologies are used. PCAO shall provide control mechanisms on the use and access of these social media to avoid abuse of the service.

2.7 Electronic Records Management and Archiving

The preservation and access to electronic records, including web based resources, shall be planned so as to ensure availability and access throughout the life of the record. MDAs shall adopt best practices in records management for web resources. These may include:

- Identifying records that exist on their websites and those that need to be placed online

- Ensuring that full and accurate records of web resources are captured and maintained for as long as they are required
- Providing online access to electronic records and archived information in the relevant format
- Capturing full and accurate records of web based transactions into a record–keeping system that can guarantee the authenticity, reliability and accessibility of the records

Where MDAs have database records online, special care shall be taken to ensure that proper authentication mechanisms are used during access to various databases. There shall be standardized secure access mechanisms to Government databases. MDAs shall ensure that database transactions are adequately protected by use of passwords at personal entry and business need digital signature shall be used. Guidelines shall be put in place to administer and manage databases that are accessible through the MDA website.

2.8 Metadata

Metadata is structured data that describes the characteristics of an information resource and its intellectual property rights. Metadata is a vital tool for managing and providing access to electronic resources. MDAs shall use metadata to describe their web based information to improve the visibility and discoverability of those resources via web based search facilities. Metadata also will be important for preserving and managing electronic records and ensuring their continued accessibility over time. MDAs are required to apply the generic metatags – 'keywords' and 'description', which are indexed by the majority of commercial search engines. MDAs are encouraged to use as many additional metadata elements as are necessary to enhance their resource description and maximize discovery. There shall be Government metadata to support Government customized search engines.

2.9 Web Security and Privacy

The use of the Internet platform comes with inherent security threats and risks. As reliance on cyber space continues to increase, so do the number and complexity of associated security challenges. MDAs shall, as a matter of necessity, put measures or controls to protect web resources to assure the confidentiality, integrity and availability of information. The MDAs need to be confident that their information assets are safely and securely stored, processed, transmitted and destroyed.

In securing their web content, the MDAs shall develop website security plans in accordance with the e-Government Security Policy. MDAs shall ensure that users are alerted of potential risks and how to avoid them when accessing the website.

Where MDAs solicit or collect information from users through electronic forms or email, they shall ensure that this information is securely transmitted and stored by taking appropriate measures such as data encryption. Further, where MDAs need to transmit information to users, they shall ensure that the information is protected through appropriate technologies. Reasonable care shall be taken to protect the personal information held by an MDA from misuse, loss and unauthorized access, modification or disclosure. Where necessary, user registration for access and use of services such as access to government databases shall be enforced.

As a best practice, MDA websites shall include a standard privacy policy statement that enumerates information collected about individuals when they visit the website, how it is used and if it is disclosed. It is important that an MDA complies with the undertakings and representations in its website privacy statement.

MDAs shall regularly conduct security threat and risk audits on their websites. They shall also create and regularly review a security plan that describes the necessary security mechanisms and procedures.

2.10 Hosting and Web Services

MDA websites and their domains shall be hosted within government ICT infrastructure. Government web hosting shall aim to ensure the high availability of websites, databases, applications and services. Government web hosting shall provide for secure remote access through ftp and a control panel, to enable uploads to the web server.

MDAs shall manage their web hosted applications through a secure management tool that provides control, flexibility and reliability. There shall be regular back-ups of all hosted content for the purpose of ensuring business continuity in case of failure. MDAs shall also develop a comprehensive business continuity and disaster recovery plan.

For content that requires to be hosted outside the government ICT infrastructure, for example video on YouTube, approval needs to be sought from PCAO.

2.10.1 Hosting Service Requirements

Government hosting services shall meet the following minimum requirements:

- The services shall be provided on government owned and managed web, application or database servers and will run on a common platform to facilitate ease of maintenance.
- Servers shall be housed in a secure, managed equipment environment
- Application switches shall ensure that appropriate levels of resources are available to cater, for seasonal loading peaks.
- A secure and private connection from the internal network shall be provided for management access
- Data replication to an off-site storage location should be provided
- Websites shall be mirrored to provide continuity and the ability to share workload

2.10.2 Government Gateway

It is recommended that MDAs shall manage access to the Internet and mail services in a secure manner. The government gateway shall be secured by appropriate controls such as firewalls sitting between the Internet and the MDA's local area network, where hosting is at the MDAs premises. The quality of this service shall be built around the principles of secure computing, premises, processes and qualified personnel.

The Government gateway shall provide mechanisms for authentication, access control and encryption in order to protect systems and information at the Internet boundary. In addition, operating system configuration on the web server shall provide another layer of protection. They include:

- Privilege reduction – The web server shall be run as a non-privileged user, with limited access to system resources
- File system limitation – The web server shall have limited or no access to the host server's file system.
- Limited interactive system – All non-administrative users shall be removed from the computer that runs the web server to reduce the risk of circumventing any web server access controls
- Data and command validation – There shall be validation of expected data and command strings
- Creating a sterile environment – Unnecessary services, files and executables shall be removed from the web server environment to deny attackers any potential opportunity to bypass established security
- Monitoring network and server audit logs

2.10.3 Web Server Statistics and Reporting

The Government web hosting solution shall provide statistics on page visits, unique visitors, successful and unsuccessful requests, most and least frequently visited pages, most common entry pages, top referring sites and search terms used.

Webmasters shall retain server logs and ensure that statistics are available across the MDA for business planning. Reporting shall be done frequently as required by all for enhanced decision-making on the following among others:

- Additional bandwidth
- Differential management for international and national traffic
- Additional disk space
- Additional software
- Maintenance of any hardware provided

2.11 Website Promotion

The Web Management Unit and MDAs shall prepare promotional plans for the Government Portal and MDA websites. Web addresses and email addresses shall feature as part of the medium used in conventional advertising and promotion. Promotion plans shall address the following:

- Conventional Advertising and Promotion – These shall include:
    - Press – Advertisements and editorial
    - Direct mail – Letters, flyers, brochures, newsletters
    - Television and radio exposure
    - Public meetings, seminars
    - Business cards, letterheads and other stationery

- 'Website discoverability' – To achieve this, indexing agents require:
    - Using meta 'description' and meta 'keyword' tags
    - Placing a brief summary of keywords at the beginning of websites
    - Creating descriptive, carefully worded titles
    - Using keywords throughout the documents
    - Registration with the major international search engines
- Internet Avenues – Different electronic options including:
    - Email – An email list of consumers
    - Links – Link to other MDA websites and the Government Portal
    - Request shall be sought to provide pinks to Private sector and other non-governmental organizations
    - Maintain news groups and mailing lists

CHAPTER 3

NETWORK INFRASTRUCTURE MANAGEMENT

3.1 Introduction

This chapter provides guidelines for design, development, utilization and management of the Government Network Infrastructure (GNI). It focuses on the standards and guidelines that support the development and progressive growth of GNI.

The main objective of these guidelines is to provide coherent, coordinated and consistent development of a shared GNI as well its operationalisation and optimized utilization.

The GNI shall serve as the ICT Backbone for linking and inter-connecting MDAs across Government. The GNI is intended to:

- 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 chapter also take cognizance that after a decade of development and platform integration, IPv6 stands ready to revolutionize the Internet, networking, and the telecommunications industry. Upon complete exhaustion of the IPv4 address space in 2012, new devices and networks will be unable to obtain IPv4 addresses and will therefore need to use (IPv6).

3.1.1 Audience

These Guidelines shall be used by Government of Kenya Ministries, Departments and agencies. The GNI guidelines are aim to be inclusive to all users, bearing in mind the wide range of user circumstances, computer capabilities, technical knowledge and interests. MDAs in consultation with DeG shall carry out site surveys, design, implement, optimize, and operationalize the GNI.

3.2 GNI Architecture

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

- **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.

- **Campus Infrastructure** that shall consist of communication systems between groups of buildings within a larger geographical area. Campus Infrastructure typically interconnect disparate communities of interest for information sharing and interoperability using private facilities or public carrier communication facilities.
- **Wide Area Networks** that shall consist of communications systems that span a very large geographical area. WANs shall interconnect distributed GoK facilities and also may function as aggregation mechanisms for disparate MDAs with common communication requirements. WANs shall typically use or provide public carrier communication facilities.
- 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 primarily be located at the GDC providing centralized resources for server management and data storage. The Netwojrk Management Team at the NOC shall provide support for both local and remote locations.
- 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.
- GNI Architecture shall also include but not limited to: Servers and associated storage devices, Environment and Power control equipment, bandwidth Management equipments and telecommunication devices such as Data Terminal Units (DTUs), modems.

3.2.1 GNI Architecture General Principles

The planning, design and development of the GNI Architecture shall be guided by the following general principles that support GoK's strategic business goals and objectives. The GNI shall:

- Provide the infrastructure to support GoK business and administrative processes
- 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 governemnt services.
- MDAs shall use standard devices and architecture approved by GoK.

3.2.2 GNI Guidelines

All MDAs connecting to the GNI shall interconnect using the acceptable international standards. These include but not limited to:

- International Organization for Standardization (ISO)
- Institute of Electronics and Electrical Engineers (IEEE)

- International Telecommunication Union–Telecommunication standardization sector(ITU-T)
- Electronic Industries Alliance (EIA)
- Telecommunication Industry Association (TIA)
- American National Standards Institute (ANSI)
- European Telecommunication Standards Institute (ETSI)

3.2.3 GNI Guidelines Statements

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:

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

Table 1: Standard Details

<table>
<tr><td rowspan="7">Physical Media</td><td colspan="2">Description</td></tr>
<tr><td colspan="2">Cabling and plugs</td></tr>
<tr><td>Classification</td><td>Technology Component</td></tr>
<tr><td>Emerging</td><td></td></tr>
<tr><td>Current Standard in Use</td><td>Fibre Single/Multi Mode Optic Fibre, UTP(Cat 6/6a), Structured Cabling System, Coaxial cable</td></tr>
<tr><td>Legacy</td><td>UTP (Cat 5e), Telephony UTP (Cat 3/4</td></tr>
<tr><td>Antiquated</td><td>UTP (Cat 3/4</td></tr>
</table>

<table>
<tr><td></td><td colspan="2">Standards</td></tr>
<tr><td></td><td colspan="2">• AS/NZS 3080 Telecommunications Installations – Integrated Telecommunications Cabling Systems for Commercial Premises
• AS/NZS 3084 Telecommunications Installations – Telecommunications Pathways and Spaces for Commercial Buildings
• AS/NZS 3085.1 Telecommunications Installations – Administration of Communications Cabling Systems Part 1: Basic Requirements
• AS/NZS 3086 Telecommunications Installations – Integrated Telecommunications Cabling Systems for Small Office/Home Office Premises, SAA HB 29:2007 Communication Cabling Manual AS/ACIF 5008 and 5009
• TIA/EIA 568, 569A, 606, 607
• Fiber SM ITU-T G.652 (non-WDM), ITU-T G.652.C (WDM un amplified metro access)</td></tr>
<tr><td>Routing/Switching</td><td colspan="2">Description</td></tr>
<tr><td></td><td colspan="2">A routing/switching protocol shall manage the movement of information around the network</td></tr>
<tr><td></td><td>Classification</td><td>Technology Component</td></tr>
<tr><td></td><td>Emerging</td><td></td></tr>
<tr><td></td><td>Current Standard in Use</td><td>Multi-protocol label switching (MPLS), IPv4, IPv6, BGP/iBGP, OSPF, IGMP, PIM, MBGP, EIGRP, HSRP, VRRP, ISIS, SSH, SSL, DHCP, Telnet, NTP,VPN, TCP, UDP,DNS,FTP, HTTP,</td></tr>
<tr><td></td><td>Legacy</td><td>RIP</td></tr>
<tr><td></td><td>Antiquated</td><td>IPX/SPX</td></tr>
<tr><td></td><td colspan="2">Standards</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Technologies – Transmission</td><td colspan="2">Description</td></tr>
<tr><td></td><td colspan="2">A transmission protocol shall standardize means of information transfer across a network. Both sender and receiver must use the same protocol for data to be received and interpreted as intended by the sender</td></tr>
<tr><td></td><td>Classification</td><td>Technology Component</td></tr>
</table>

	Emerging	
	Current Standard in Use	MAC, 802.3x,10 Giga - Ethernet, Giga – Ethernet, Fast Ethernet (100Mbps/1Gbps/10Gbps), PPP, ARP, RARP,L2TP, STP, Coarse Wave Division Multiplexing (CWDM), Dense Wavelength Division Multiplexing (DWDM), 802.3af Power over Ethernet (PoE), VLAN (IEEE 802.1Q), VTP, E1, DSL, Ether Channel, STM1,STM4,STM16
	Legacy	802.3 Ethernet (10Mbps), Asynchronous Transfer Mode (ATM), x.21, v.35
	Antiquated	
	Standards	

Data Network Devices	***Description***	
	A Data Network is a system for communication between computers. These networks may be fixed (cabled, permanent) or temporary, via modems or null modems.	
	Classification	***Technology Component***
	Emerging	
	Core	Active Devices that is Layer 2 and 3 switches, Layer 3 routers shall support routing/switching and transmission technologies
	Legacy	
	Antiquated	Un Managed Switches, hubs
	Standards	
	IPv6 compliant	

Network Management	***Description***
	Network Management, typically applied to GNI refers to the maintenance and administration at the top level. Network Management software tools shall implement functions required

	for controlling, planning, allocating, deploying, coordinating and monitoring the resources of a network.	
	Classification	***Technology Component***
	Emerging	
	Current Standard in Use	Simple Network Management Protocol (SNMP v2.0 and v3.0), Remote Monitoring (RMON), SCADA, SYSLOG, ICMP,
	Legacy	SNMP v1.0
	Antiquated	
	Standards	
	IPv6 compliant	
Protocol / Multi- media	***Description***	
	A protocol is a set of rules that both the sender and receiver of a Media message must follow in order for the message to be received and interpreted correctly. A multi-media protocol shall provide a service or function to a multi-media application	
	Classification	***Technology Component***
	Emerging	SOAP
	Current Standard in Use	VoIP: IETF Session Initiation Protocol (SIP) with Session Description Protocol (SDP), Session Announcement Protocol (SAP), Real-Time Streaming Protocol (RTSP), Video: ITU-T H323 Videoconferencing Protocol, H.460 (H.323 Traffic) Firewall Traversal, Real Time Protocol (RTP), CSTA, Fax over IP, Protims, FCCS, CCIS, SS7
	Legacy	E&M, TAPI
	Antiquated	
	Standards	

Technologies Firewall/Security	***Description***	
	A firewall/security protocol shall manage the security of information around the network	
	Classification	***Technology Component***
	Emerging	
	Current Standard in Use	Network Address Translation (Dynamic DNAT, Static NAT), Secure Socket Layer (SSL), Secure Shell (SSH), Transport Layer Security (TLS), Secure Multipurpose Internet Mail Extensions (S/MIME), Application Detection Vulnerability Language (AVDL), 3DES, AES, GRE, IPSec
	Legacy	PPTP
	Antiquated	
	Standards	
Radio Network	***Description***	
	A GNI shall supports mobile operations, such as police, prisons and other emergency services, via radio communications as well as other forms of transmission such as microwave.	
	Classification	***Technology Component***
	Emerging	
	Current Standard in Use	RDLAP (GRN), Smartzone (GRN), FLEX (GRN), DECT, IP, SDH, PDH, APCO16, P25
	Legacy	
	Antiquated	
	Standards	
Transmission – Carrier	***Description***	

	GNI shall support transmission Technologies to interconnect communication devices.	
	Classification	***Technology Component***
	Emerging	Fibre to the Node (FTTN
	Current Standard in Use	PSTN, Frame Relay, Asynchronous Transfer Mode (ATM), Digital Subscriber Line (xDSL), Ethernet 802.3, PRI-ISDN, IP, SDH, PDH, Carrier-IP (generic)
	Legacy	Legacy 2Mb G.703, BRI-ISDN, PAPL
	Antiquated	FDDI, VGDL, DDS Low Speed
	Standards	
Wireless Network	***Description***	
	GNI shall support technologies that provide access to mobile data devices	
	Classification	***Technology Component***
	Emerging	802.15 Wireless Personal Area Networks (WPAN), 802.16
	Current Standard in Use	802.11a, 802.11b, 802.11n, 802.11x, Bluetooth, Wireless Security (EAP, WPA2, 802.11i),
	Legacy	WAP Datagram Protocol (WDP)
	Antiquated	WEP, WPA.
	Standards	

Fixed telephony devices	***Description***	
	A network that encompasses fixed-line telephony services	
	Classification	***Technology Component***
	Emerging	
	Current Standard in Use	VoIP PABX, VoIP SoftSwitch, Small Business System (SBS)
	Legacy	TDM, PABX
	Antiquated	
	Standards	
	IPv6 compliant	
Mobile Telephony/ Mobility	***Description***	
	A network used to communicate voice/video/data wirelessly. Other mobility device covered under Mobile Phones and PDAs /Wireless Devices	
	Classification	***Technology Component***
	Emerging	4GSM
	Current Standard in Use	SMS, MMS, 3GSM, Push to Talk, LBS, CDMA
	Legacy	2GSM,
	Antiquated	
	Standards	

3.2 Management of GNI

3.2.1 Connectivity Requirements

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

i. To conform to defined open standards and GoK standards
ii. To provide documentation for user and technical manuals
iii. To regulate connections at the network level utilizing access control mechanisms and rights

iv. All connections within GNI shall be based on a standard speed determined by the DeG.
v. The GNI shall be built on the IP/MPLS
vi. The MDA shall set-up a VPN before getting access to the GNI
vii. The MDAs LANs terminations equipment to GNI shall be provided by DeG
viii. The connection technologies supported are, ADSL, ATM, STM, Leased connections, T1/T3, E1/E3, Serial, Frame Relay and Ethernet
ix. MDAs shall ensure interoperability of all active devices with GNI

3.2.2 Connection requests and approvals for GNI

In general, network services provided over the GNI shall be granted by the DeG based on MDAs needs. Such needs shall be requested in writing by a senior officer.

The DeG shall issue, certify and revise GNI connectivity requests, standards and compliance mechanisms. At all times, the Government through DeG shall retain governance on any connection in operation. Thus,

- 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 organizations;
- Every MDA 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.
- IP addresses allocation for the connection link and associated equipment shall be administered by DeG

3.2.3 Suspension and Termination of Connection

The DEG shall maintain 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 authorization by DEG.

3.3 Network Management Team

The DeG shall establish a Network Management Team to responsible for the GNI. This team shall consist of Network Administrators, System Engineers and Security Experts. Its responsibilities shall include:

- Monitoring Network activities
- Implementing Network Security policy
- Perform network control functions to ensure maximum network security
- Accept and resolve all network operations escalations for the GNI
- Advice management on emerging Network Technologies and procurement
- Perform Network operations and Administration activities to ensure maximum availability
- Carry out corrective network activities to restore network availability

- Undertake Network Support activities to ensure timely faulty repairs and network service restoration
- Update documentation of network operations method of procedure

3.4 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 changes requests.

GNI equipment configurations of the components shall need to be documented for the purpose 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 DeG.

3.5 Network Security

Network Management Team in conjunction with the MDAs Network Administrators shall oversee the security of GNI and MDA networks respectively. To maintain the highest level of security surveillance on network performance shall be maintained at all times in order to ensure optimized network availability 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 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.

3.5.1 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 encrypted. Additionally, detailed logging shall be provided in accordance with acceptable security recommendation of all transactions and user driven events on the GNI including:

- Individual user access, login and log-off
- Changes to system and monitoring configuration
- Addition or deletion of devices
- Changes to policies, alerts and notifications
- Access to reporting and other system functions

3.5.2 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:

- Configuration management
- Reporting
- Discovery
- Policies
- Workspaces
- Management and monitoring of services, servers, applications and devices

3.5.3 File exchange via FTP

With the use of router Access Control Lists (ACLs), file exchange via ftp shall take place to/from designated ftp servers, only.

3.5.4 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 MDA'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.

3.5.5 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.

3.5.6 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.

3.5.7 Protection of Information and Network Resources

The DeG shall be responsible for ensuring that all possible measures have been taken to ensure the integrity and privacy of the government confidential information. MDAs 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:

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

3.5.8 Physical Security and Entry Controls

The Network Management Team in conjunction with the respective MDAs 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 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:

- Hazardous materials shall be stored safely at a safe distance from the site. Combustible material such as stationary shall not be stored within the computer room until required.
- 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.
- Appropriate safety equipment shall be installed in accordance with the Occupational Safety and Health Act.
- Emergency evacuation procedures shall be developed with due consideration of the security of the ICT resources.
- Environmental requirements of an equipment room shall be determined by Manufacturer's specification with due diligence and in consultation with certified professionals.

3.5.9 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 consultation with Ministry of Public work and Communication Commission of Kenya (CCK).

3.5.10 Power Sources

Information resources shall be reasonably protected from power failures or other electrical anomalies such as power surges or dips, MDAs 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.

3.5.11 Management Information and Audits

The 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:

i. Authentication database showing the specific login entries;
ii. All entity router/network device configurations;
iii. Client equipment where tampering may be reasonably suspected;
iv. Bandwidth management;
v. Monitoring of access points;
vi. Monitoring dash boards; and
vii. Monitoring unauthorized use of network and network facilities.

The Network Management Team shall investigate any unauthorized changes immediately. All MDAs connections shall be reviewed on regular basis, by mutual agreement. The Network team shall come up with and document routine maintenance processes. The team shall come up with SLA for maintenance of network resources with external service provider and ensure that they are adhered to.

CHAPTER 4

SOFTWARE GUIDELINES

4.1 Introduction

Software is a set of programs, procedures, algorithms and documentation that instruct the computer how to carry out specified functions. The standard provides and prescribes best practices for software development, acquisition, support and maintenance by MDAs. These best practices have been recognized to significantly contribute to the successful acquisition, deployment and utilization of software systems.

Software guidelines and standards shall aim to assure software quality, ensure software internal usability, and help evaluate the software product. Their application by the DeG aims at achieving the following objectives:

- Ensure data/ information sharing across Government;
- Enhance user satisfaction;
- Ensure compatibility;
- Enhance unified support and management;
- Reduce cost and improve savings;
- Offer a unified training for programmers;
- Improve staff productivity; and
- Ensure coherence in upgrade management.

In addition, when deploying software the MDAs shall ensure conformity to International Software Standards. The acceptable software international standards in this case include:

- ISO 9126- 1 on Software product quality
- ISO/IEC 9126-2 on External usability metrics
- ISO/IEC 9126-3 on Internal usability metrics
- ISO/IEC 9126-4 on Quality in use Metrics
- ISO 9241-11 on Guidance on usability
- ISO 14598 – 1 on Software product evaluation.

The guidelines shall publish acceptable standards for software products bought off-the shelf, Free and Open Source Software (FOSS), software developed internally or developed by contracted third parties. For the purpose of this guideline, software is classified in three broad categories based on its purpose, functionalities, type, or area of application.

1. Application software.
2. System software.
3. Application Development software.

It is also important to note that most of the systems in MDAs should be upgraded to support IPv6. An audit should be conducted to establish the IPv6 readiness in MDAs.

4.2 Application Software

Application software refers to computer software designed to perform a specific task or a specific set of tasks.

Acquisition of application software, unlike other types of software shall require an elaborate approach due to nature of it specialization. Since applications shall be acquired for a diverse business processes and support services, the procedures guiding this acquisition shall be determined by the nature of the application as well as availability in the market of off-the-shelf programs that address the specific business requirements. In all application software acquisition procedures, a technical committee comprising of business and ICT subject experts is presumed. In addition, application of a standard software development methodology and project management guidelines shall be enforced.

Acquisition of application software shall therefore fall under the three broad procedures:

4.2.1 **In-house Development:**

All In-house development of business software shall be coordinated by the DeG. The software development process will adopt a project management approach. The DeG will constitute a development team consisting of various specializations as may be required in specific software development task. These shall include software developers with expertise in target development platform, business/systems analysts, business/systems designers, database experts, network and communication, security specialist among other skills that may be required in different project.

4.2.2 **Outsourced Development:**

For sophisticated system development initiatives that require skills and knowledge not available within DeG, an external developer may be contracted to deliver the business application. In this case, the implementing agency in collaboration with DeG will adopt a project and constitute a technical team consisting experts in the business process, business/systems analyst and the relevant ICT skills. Depending on the complexity of the anticipated system, the technical team will:

a) Develop a Request for Proposal including well articulated and comprehensive business and functional requirements that well informs a contractor to enable submission of proposal that delivers a turn-key business solution.

b) Develop a detailed design including specifications of user requirements, specifications of the software, hardware, communication and networks as well as other software development services. The process of implementation could then phased and sourced from experts on specific system aspects.

4.2.3 **Commercial off-the Shelf:**

In some cases, a project technical team having developed the business and functional requirements in software development process may seek to acquire a solution that is readily available in the marketing. Examples of such solutions include modules of ERP software. In this case the technical team must ensure that the business, functional and technical specifications are well articulated in order to avoid any ambiguity that may lead to the solution not meeting all the requirements or a solution becoming impossible to implement.

4.3 Systems Software

System software refers to computer programs used to start and run computer systems and networks, often called Operating Systems.
MDAs shall endeavor to upgrade, to the minimum requirements, all software that fall below the recommended standards. MDAs shall ensure that:

i. Licenses for commercial operating system are provided upon acquisition, duly registered and subsequently renewed as per the requirements of the copyrights;
ii. The latest stable version is purchased in each case;
iii. Vendor Support is provided;
iv. The software is regularly updated with the latest patches.

ICT units shall keep an inventory of all operating system software installed and closely monitor and evaluate to ensure licensing and copyright agreements are maintained. The head of the units shall take custody of all Operating System software installation materials, including manuals where supplied. They shall also ensure that where possible, back-ups are carried out before any reinstallation or upgrade of an operating system. The units shall organize training for users on any new client operating system software.

4.4 Application Development Software

Application development tools such as compilers and linkers, used to translate and combine computer program source code and libraries into executable programs.
MDAs shall ensure that ICT officers responsible for development of software are adequately trained on all application software acquired.
MDAs shall take into consideration the following when acquiring application development software:

a) Type of application to be developed; Desktop application, Web based application or server application.

b) Operating System platform the software to be developed is to run on.
c) Integration with the existing systems.
d) Database to be used by the application.
e) Compatibility with existing and future hardware and software platforms.
f) Speed of development.
g) Performance of compiled code.
h) Assistance in enforcement of code
i) Portability; can the application developed be used in an operating systems other than the one in which it was created without requiring major rework.
j) Fitness of the software for the application being developed.

4.5 Software Acquisition

4.5.1 Commercial Software

Commercial Off-the Shelf Software (COTS) refers to ready-made software installed on Government information technology systems or acquired by Government agencies through initial purchase or upgrade, including leased software, shareware and freeware.

COTS software configurations must be based on Government requirements. All COTS software that meets the e-Government configuration and support standards will be maintained by the Ministries concerned. Where a particular version of a COTS software product is specified, unless there is a justification otherwise, it is recommended that this version not be the latest available. This practice minimizes the risk of error-prone software. However, the justification for specifying a particular version of COTS software is the discretion of the Ministries.

The e-Government COTS configuration standards are sufficiently flexible to adapt to changing business and service needs and are developed in the context of the Government-wide infrastructure as well as the e-Government strategy.

The Directorate of e-Government periodically reviews and updates, if necessary, these COTS Software configurations standards on an annual basis, but more frequently if the circumstances warrants. The updates follow the same review and implementation process as described above.

4.5.1.1 Minimum Requirements for Commercial Software

Below are the minimum requirements that must be considered in the acquisition of COTS:

- **Total lifecycle cost**. This cost includes initial costs such as purchase, installation and training, plus the on-going cost of maintenance and support.

- **Maintainability**. This criterion addresses the ability to administer and perform corrective, adaptive or perfective maintenance on the COTS product within defined tolerance for cost and service, using vendor and/or internal support. This criterion includes minimal operational disruptions and downtime, the ability to tune the software to improve efficiency

and effectiveness and the cost and effort to upgrade to improved versions of the software product.

- **Interoperability.** This criterion seeks to minimize the additional support required to integrate the COTS product as a functioning component in the State IT portfolio. As an example, the exchange of information between potentially heterogeneous systems can be facilitated through open standards or non-proprietary protocols (e.g., TCP/IP). Interoperability should include flexibility in supporting changes over time and among multiple state agencies and systems. Interoperability standards affecting more than one Agency will be mutually determined and consistent with all higher-level (e.g., Statewide) standards.

- **Portability.** This criterion addresses the ability of an existing software component to move from one physical or logical position in the IT infrastructure with minimum impact on cost and service.

- **Scalability.** This criterion ensures that acceptable COTS software products enhance the ability of the system to support future growth and increased throughput necessary to meet e-Government goals. This objective is achieved through excess capacity or the flexibility to easily modify and/or enhance the system as needed (e.g., application performance or transaction process speed, forward and backward compatibility, modularity, etc.).

- **Availability/Accessibility.** This criterion seeks to maintain a system's operational readiness and required level of service without disruption from software failure. This is achieved through robust and/or redundant (e.g., fault tolerant) software. Operational readiness will include the ability of users and operators to access the system, in a timely fashion, to perform its intended functions.

- **Reusability.** This criterion addresses the ability to make repeated use of the COTS software product for additional requirements with minimum additional cost.

- **Functionality/performance.** This criterion seeks to guarantee that the e-Government Operational requirements, especially its mission critical requirements, intended to be performed by IT systems, can be achieved effectively and efficiently with the specified COTS software. It includes the properties of efficient software/hardware integration that affects the ability of the overall system to perform adequately to meet operational requirements.

- **Security.** This criterion addresses the need to protect system data and the operational environment from loss or compromise. It includes the ability of the COTS software to prevent and contain malicious as well as non-malicious security breaches.

- **Other Specific Criteria.** Other criteria are explicitly used for specifying the acceptable set of COTS software products. For example, vendor viability, licensing restrictions, potential

product market share, customer recommendations, and product volatility (e.g., frequency of upgrades and potential obsolescence) may be important.

The following configurations are defined as the acceptable COTS software for e-Government - based on an analysis of our requirements:

4.5.2 Off the Shelf Software

Off-the-shelf or commercial software defines software which is ready-made and available for sale, lease, or license to the general public. Purchasing a commercial off-the-shelf software solution requires attention to technical and cost considerations.

The correct solution shall weigh heavily on the ICT Staff and the MDAs who shall:

1. Identify and research specific products that could support our recommended solution for the target information system.
2. Solicit, evaluate, and rank vendor proposals.
3. Select and recommend the best vendor proposal and why.
4. Contract with the awarded vendor to obtain the product.

4.5.3 Open Source Software

Open software enables access to the source code written in the programming language in which the special-purpose programme is written, which allows the expert users to read, modify and adapt the open source software to current purposes. Open software is at the same time a computer programme whose source code may be freely redistributed, modified and connected with other software based on an open code.

Open software is based on the principle of freedom to use, redistribute, complete, improve/upgrade and subsequently distribute the software. This freedom of software use enables interested parties to perform joint operations in improving or extending software functions without the pressure of a proprietary relation, which prevents this type of cooperation. This form of cooperation (Community) in which experts from different sectors and organizations, even from different countries, work jointly in creating, developing and using software, is called the system of Open Source Development.

4.5.3.1 Use and development of Open Source Software

The following considerations are made for the use and development of open software within the MDAs:

- To treat open source software and proprietary software equally. In all the procedures of software development and procurement, the choice shall be based on the financial and functional properties of certain software regardless of the existing business relations or model in use.

- In developing information systems, MDAs shall to the greatest possible extent develop, create and procure software based on the use of open standards.
- Avoid the use of software which is difficult to interface with other software or data exchange between software of different information systems in MDA. In cases where this is not possible due to closed nature of the legacy software, all subsequent upgrading and modifications in these systems shall have to be based on the support of open source software and open standards. This will enable the connecting of information systems across Government.
- When it is economically or financially justified, request from the supplier full ownership and the right to use and distribute the source code of procured software. The Government shall put to public use the software for which ownership was obtained and software whose creating was financed form the budget funds, together with the licenses obtained with the procured software.
- When it is financially, economically and technologically justified, advocate a more widespread use of open software in state administration bodies and other budget beneficiaries alike. Along with supporting open software, the Government shall also attempt to achieve as favorable and acceptable market, financial and other terms of use of the proprietary software in state administration bodies.
- Promote software development based on the open source and it shall promote integration of open software and open standards in the process of developing the existing information systems in GoK agencies. Through these actions, the Government shall promote the development of domestic proprietary software based on open standards.
- Support the training of civil servants to use open software and it shall promote the development of materials used to educate civil servants in the area of open software and open standards.
- Promote integrating the knowledge related to the software solutions based on the open source into educational programmes. In the process, contents on the open and proprietary software shall be presented equally in order to prepare the younger generations for independent decision-making on the choice and legitimacy of the chosen software for individual information and business purposes.

4.6 Application software acquisition guidelines

4.6.1 Office Productivity

Office productivity software refers to a collection of programs for a personal computer that are used to automate common office tasks. The packages usually include: word processing, spreadsheets, presentation applications, email, and database. These components are sold together and typically interface with each other.

MDAs shall ensure that:

- The latest stable versions of office productivity suites are installed in user computers and that security and software updates are made as soon as they are released. Where a previous version is to be used adequate justifications are to be provided.
- Users are adequately trained on the use of any office productivity suites purchased.

- All office productivity suites acquired is adequately supported and maintained by the vendor.

4.6.2 Utility Software

Utility software is refers to system software designed to help analyze, configure, optimize and maintain the computer.

MDAs shall ensure that all computers and servers are installed the minimum utility software. These include and are not limited to:

a) Disk Defragmenters
b) Registry Cleaners
c) Backup Utility Software
d) Data Recovery
e) Antivirus Utility Software

ICT units shall ensure that:

- Back up is carried out before running any defragmenting or registry cleaning software.
- Utility software is compatible with existing operating systems before installation.
- Running of any utility software for system maintenance does not interfere with users operations.
- Monitor the use of utility software to prevent against loss of user information and system damage.

4.6.2.1 Security Software

Security software protects the operating systems, network and data from risks and threats to their confidentiality, integrity and availability. Security software ensures that threats and risks associated with the use of computers are managed or mitigated to acceptable levels for enterprise productivity. Due to high risks in a networked environment, MDAs are obligated to implement basic security software to protect information held or transacted.

To adequately cater for their security requirements, MDAs shall implement security software deemed appropriate from the following proffered set:

- Endpoint protection systems (AntiVirus, AntiMalware)
- Firewalls/intrusion detection & prevention systems
- Identity and access management systems
- Physical surveillance & monitoring systems
- Encryption systems
- Enterprise information security management
- Network service management systems

- Security auditing, assessment and remediation systems
- Privacy monitoring systems
- Disk storage, recovery, and anti-forensic systems
- Digital forensics systems
- Penetration and fuzzers

The security requirement will be defined for each MDA in order to ensure data is safeguarded and appropriate level of security deployed to conform to legal and contractual mandate of the MDA.

4.6.3 Web Development and Management Software

A number of FOSS for web development and management are freely available. Where a MDA chooses to use FOSS it is encouraged that software updates made more regularly. Commercial Content Management Software may however, be acquired in accordance with laid procedures for commercial software.

All web management software shall conform to the Web Development and Management Guidelines.

4.6.4 Database Software

Database software refers to all software used to allow users input, retrieve, analyse and generate report of data or information.

MDAs shall ensure that all database software has and is not limited to the following features:

- Scalable; to accommodate the growing number of transactions.
- Data visualization; the software should enable one to analyze data and information graphically of in raw streams.
- Performance; the database software should be able to efficiently utilize just about any reasonable hardware platform on which it runs. It should also be able to manage multiple high-speed processors, clustered servers, high bandwidth connectivity and fault tolerant storage technology.
- Reporting; the database software should be able to modify existing reports and create new custom reports on an ad-hoc basis to meet specific organizational management information needs both in the present and in the future.
- Extensibility; the database software should support extensibility to accommodate any necessary changes to the system in the future.

MDAs shall ensure where possible that all database software acquired support for existing systems within the MDA and across government.

MDAs shall ensure that the software license agreements to do no prohibit data integration or movement of databases across different hardware platforms.

4.6.5 Communication Software

Communication software refers to applications or programs that enable users and computer systems to exchange and share information.

4.6.5.1 Email Software

MDA's shall ensure that all corporate email software solutions acquired provide for:-

- Sending of group emails
- Creation of mailing lists from the server.
- Email search and retrieve.
- Creation of email folders.
- Email archiving.
- Global address book for all registered users.
- Sending email attachments of at least 5MB.
- Appending of a Digital Signature.
- Formatting of e-mail messages (Text formatting, appending of graphics).
- Email Account management.
- Security; Real-time spam and Junk mail filtering, password management and client/server system patching
- Adequate disk quota for all email users.
- Back up of user mailboxes.
- Push to email support for mobile devices.

All email accounts maintained by an MDA's email messaging system are property of the MDA. MDA's shall ensure that all users within their organizations are supplied with an email address. Once a user has left the organization, MDA's shall ensure that the user access to their account at the MDA is disabled.

ICT units shall ensure that emails are backed up periodically. Security of email servers shall at all times be enforced. As minimum, MDAs shall:

- Ensure that the server is protected with a firewall and Antivirus software is installed and regularly updated.
- Email transmission is secured through the use of encryption technology such as SSL or TLS among others.

All corporate email software's acquired by an MDA shall have the following features:-

- Scalability- to cater for growing number of users.
- Compatibility- with different client operating system environments.

The protocols that shall be supported by email solutions acquired by MDA's shall include but not limited to SMTP, MIME, POP3, IMAP4, LDAP version 3, , SSL , TLS and Secure MIME.

4.6.5.2 Collaboration Software.

Collaboration Software is software enable organizations and users to share information with each other, coordinate and work together cooperatively on joint projects and assignments.

ICT units within MDAs shall be responsible for the acquisition, installation, maintenance and support of all collaborations systems. They shall also be responsible for user account management as well as undertaking user training focusing on acceptable use these systems. Collaboration systems acquired by an MDA shall:-

- Support Features such as email messaging, IP telephony, instant messaging, personal voice service, conference call services, data conference services, document and file sharing, collaborative document and file sharing, forums, data conferencing (sharing of a white board), short message service, chat, internal bulletin, address book, video and single sign-on.
- Integrate with existing directory systems for access to contact information.
- Enable grouping of users.
- Enable a single sign on to all the services.
- Provide electronic group calendaring and scheduling.
- Project management systems to schedule, track and charts step in a project as it is being completed.
- Workflow systems to manage the collaborative flow of documents and tasks.
- Intranet portal integration.
- Support different client operating platforms.
- Support common standards for interoperability with collaboration systems in other MDAs.
- Support email push to mobile devices.

The software shall support standards related to all its components which include and are not limited to:

- Email- SMTP, IMAP4, POP3
- VOIP- RTP, SIP, H323
- Video conferencing –H323 or H320
- Directory- LDAP.
- Encryption- SSL, TLS, S/MIME

4.6.5.3 Voice Over Internet Protocol (VOIP).

Voice Over Internet Protocol (VoIP) technology is a technology that enables the transfer of voice content (both phone calls and faxes) over the Internet, an Intranet or other packet-switched network using either a dedicated IP telephone set or a networked computer running VoIP software.

Consultations with the Directorate of e-Government shall be made by MDAs in deployment of enterprise VoIP solution.

ICT units within the MDA shall be responsible for the deployment and installation of all VOIP solutions. They shall also ensure that software patches for VoIP servers and other IPT devices originate from the system manufacturer and are applied in accordance with manufacturer's instructions.
To ensure compatibility and interoperability, MDA's shall ensure that all VOIP equipment shall employ adopt commonly used protocols standards which include;

- H.323 or the Session Initiation Protocol (SIP) signaling protocols that sets up, maintain and terminate a VoIP call.
- Media Gateway Control Protocol (MGCP) that provides a signaling and control protocol between VoIP gateways and traditional PSTN (Public Switched Telephone Network) gateways.

MDA shall ensure that all VOIP communications and systems are secured by ensuring:

- H.323 protocol is secured by using TLS and S/MIME encryption for SIP.
- Adequate physical security is in place to restrict access to key VoIP servers and components.
- Firewalls designed for VOIP protocols are employed to secure the VOIP systems.
- VOIP Terminals are secured through password authentication and user authorization. User accounts shall be administered and managed by the ICT units.
- WiFi Protected Access (WPA) where mobile units are to be integrated with the VOIP system.
- Disabling of HTTP and Telnet services
- Where softphones are used, PCs should be adequately secured to protect from worms, viruses, and other malicious software.
- Creating awareness to users on how to secure use VOIP systems.

MDA's shall ensure where possible that end-to-end encryption of the VoIP conversations is employed. VoIP Services must ensure Quality of Service to main the sound quality of conventional phones.

ICT units shall document and maintain an inventory of authorized VoIP instruments and shall ensure that the VoIP systems only register and use authorized terminals. To avoid use of VOIP facilities by unknown terminals or PCs, MDA's are advised to employ use of device authentication through the use of MAC address.

Where possible, MDA's shall endeavour to separate voice and data traffic logically on the network due to bandwidth, security and Quality of service requirement of VOIP.

VoIP software should provide for:-

- Traditional calling features including call by name, caller ID, last number redial, hold, call waiting, call forwarding , transfer, divert, park, retrieve, voice mail, return call and call conferencing
- Call Coverage Make it easy to ensure that important calls are answered by administrative assistants or team members, via user-controlled Delegation and Team Calling respectively.
- Telephone Directory.
- Maintain Call history.
- Local Number portability, that is, ability to maintain phone numbers when one changes service provides.

Protocols that are supported include:-

- Real- Time Transport Protocol.
- Session Initiation Protocol.
- ITU-T H.323
- Media Gateway control protocol
- IPSec, TLS and S/MIME for encryption.

4.6.5.4 Mobile Messaging Software Standards

Mobile Messaging software shall enable MDA to send SMS to customers or stakeholders from a Computer.

MDA's shall ensure that Mobile Messaging software acquired have the following minimum features:-

- Mobile Automatic filters-To sort inbound messages into appropriate response categories to ensure that text messages that are received are acknowledged in some form.
- Address Book- store names, mobile numbers and notes. The database shall reside behind a highly secure firewall. Message History with status reports –keep a log messages and their status.
- Group Messaging - The software should setup of groups in the address book and enable sending of SMS to everyone in that group
- Report- The software should enable creation of reports and export to other documentations software's for report creation
- Bulk Messaging - This feature allows you to send an individual message to multiple
- Purge Failed Numbers- Allow MDAs to purge numbers based on a chosen number of consecutive SMS delivery failures.
- Scheduling- Allows MDAs to send out the messages at a chosen date and time. Setup recurring and automated messages to be sent out at certain days and times of the week, month, or year
- Compatibility Support for all Messaging to all Phone Models.
- multi-part messages- to allow messages longer than 160 characters

- Support for Unicode- To support extended characters that are not supported by your native character set
- Support for WAP Push messages and Flash messages
- Support for traffic limitations and throttling

MDA's shall clearly articulate the requirements for identity confirmation upon registering for a service and apply appropriate measures to ensure the validity of a customer's identification. MDA's shall ensure that personal contact details are stored securely and that contact lists are up-to-date by reviewing contact databases on a bi-annual basis

MDA's shall include a validation step in the registration process, as confirmation of the customer's intent to receive the message.

MDA's shall maintain the anonymity of customers when appropriate, for example through the use of case numbers instead of customer names, or by indicating to the customer that more information can be accessed through other means (such as email or phone). Customer and client contact lists shall be kept confidential and properly protected from disclosure.

All Messages sent shall include a message header containing the Ministry/Department sending the message and purpose of the message; body, footer on how to receive more details on the service. If the Messaging software is web based, encryption technologies such as SSL and TLS shall be employed to enforce security.

Messaging system user accounts shall be administered by ICT units within the MDA's. ICT units shall ensure strong authentication requirements are put in place. Where desktop utilities are used to send out SMS messages, the PC used to send the message should not be left unattended and must be secured using authentication mechanism such as username and passwords. Whenever inbound messages are accepted, MDAs shall respond to all inbound messages in accordance with agreed SLAs.

MDAs shall ensure that all recipients of SMS messages must have opted to receive them otherwise, seek consent from people to receive the given messages.
All messages must contain a mechanism for subscribers to opt out from further messages. MDAs shall also endeavour to ensure that users are sent messages related to the specific programme they opted into. In addition, MDAs shall maintain a record of all messaging sent or received through the messaging system.

In order to be an authoritative source of information, agencies need to make sure that their text message systems are secure. To deal with unsolicited texts (these could be queries, comments, feedback, abuse) however, MDAs shall ensure that customers steered into using a different communication channel.

4.6.5.5 Tele Conferencing /Video Conferencing

A teleconference is a telephone or video meeting between participants in two or more locations. Video Conferencing involves real-time, generally two way transmission of digitized video images between multiple locations; uses telecommunications to bring people at physically remote locations together for meetings. Each individual location in a videoconferencing system requires a room equipped to send and receive video

ICT units in MDAs shall be responsible for acquisition, evaluation, installation, set up, support and maintenance of all teleconferencing systems within an MDA.

MDAs shall ensure that all conferencing sessions are adequately secured and encrypted using standards that are not limited to SSL, TLS and S/MIME as well as through firewalls and antivirus installations. MDAs shall also ensure that physical security is enforced for all Video conferencing equipment.

MDA shall ensure that Tele/ Video conference systems are covered by maintenance agreements to ensure prompt service. It is recommended that agreements be with the manufacturer or a third-party provider who has the expertise to provide proper maintenance.

MDAs shall ensure that ICT staffs are adequately trained to use and support the Videoconferencing system.

ICT units shall be responsible for training users on how to use the Tele/Video conferencing systems.

The Corporate Video/audio conferencing software shall:-

- Support H.323 and H.320 protocol suites that are commonly implemented to ensure
- Support G722 or G711 standards for audio.
- Support for video resolutions ranging from QCIF to HD1080p
- Picture in Picture support.
- Bridging services to enable three or more parties to participate in a conference.
- Maintain a Directory of all addresses and contacts for all business.
- Integration into industry-leading desktop, workflow and IP telephony applications
- Provide for centralized Account and Password Management
- Link with existing electronic directory systems within an MDA.
- Control conferences between multiple terminals. Participant lists and rights management.
- Enable Meeting and conference recording as well as archiving.
- Screen sharing, Files sharing, notes, chat and white boarding.
- Management and administration of users.
- Polling

- Central content library
- Centralized management of the entire video conferencing network; including statistics, directories, and software updates for the system.
- End- to-end management for video conferencing endpoints and infrastructure; managing endpoints, Multiple Control Units, video and recording solutions, gatekeepers and gateways
- Should provide for adhoc and scheduled meetings and conferences.
- Integration with email and collaboration systems to schedule meetings and conference data.
- Enable for Dial in and meet me meetings.
- Moderator facility for video conferences.

All client Tele/video conferencing software installation shall be approved by the Head of ICT.

4.6.6 Network Management Software

Network management software is an application used to administer and monitor an organizations network.

MDA's should ensure that network management software acquired should be able provide the following but not limited to this features:-

- 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 events.
- Receive SNMP trap messages.
- Generate customized reports.

4.6.6.1 Bandwidth management software

MDAs shall use Bandwidth management software to optimize the bandwidth that carries traffic over networks. Bandwidth or the amount of data transferred over a communication channel in a specific amount of time shall be controlled by bandwidth management tools, or traffic or packet shapers. These tools shall enable network managers to control communications by allowing high-priority traffic to utilize more bandwidth than something given a lower priority status as well as enable them identify network traffic patterns, establish priorities, optimize application performance, and allocate resources.

As the number of Internet users shall continue to increase and demand for media-rich and peer-to-peer applications rises, bandwidth management shall continue to play a role in network management.

4.6.6.2 Network monitoring software

This is software that gathers information for management and control of a network.
The DeG shall ensure that monitoring software is in place to monitor the Government wide networks.
MDAs shall use Network management software to manage their internal networks. This software shall continuously monitor performance, events and faults. MDAs shall ensure that all Networks monitoring software can produce regular and customized reports.

4.7 Software Development

MDAs will be encouraged to develop custom software applications where necessary. Custom software or bespoke software is software that is specially developed for a specific MDA or user. It contrasts with the use of software packages developed for the mass market, commonly referred to as commercial off-the-shelf (COTS) software, or free software. Custom software can be developed by MDA in-house software development group, or be commissioned from a software house or independent software developer.

Custom software can accommodate an MDA's particular preferences and expectations. They may also be designed stage by stage to take into account all issues including those not mentioned in the specifications.

It is recommended that an optimal system development methodology such as software development lifecycle be adopted in order to obtain a useful system. In addition, a software development process must adhere to project management principles as they may be defined in the Project Management Guidelines.

4.7.1 System Development Process

The System Development process encompasses all activities involved in the development of application system. Such activities include requirements gathering, analysis, design, construction, implementation, and maintenance.

The MDAs shall use SDLC in developing applications in a well-defined, disciplined, and standard approach. It provides a methodological approach and a platform for managing, directing, monitoring and controlling the process of application or software building, including description of the process and deliverables.

Benefits of using a SDLC application/software development include:

- Has a proven successful framework
- Consistency and uniformity - methods and functions
- Results and Deliverables
- Facilitates information exchange
- Defines and focuses on roles and responsibilities
- Has a predefined level of precision to facilitate a complete, correct and predictable solution.
- Enforces planning and control

To obtain good results from the SDLC methodology, its stages must be strictly followed:

- Requirements gathering and system analysis
- System Design
- Development and Implementation
- System Testing
- Operations and maintenance

MDAs shall are required to adopt the following methodology which is derived from SDLC and outlines the specific activities in each phase as well as the outputs and deliverables of the stage.

NO	PHASE	ACTIVITIES	OUTPUT/DELIVERABLES
1	Requirements Definition	▪ Review requests ▪ Meet with Users to clarify request ▪ Modify request requirements ▪ User approval of requirements	• Understanding of request • Project Control Document • Clarified request • Requirement Document (template available) • Explicit written User approval on requirements (template available) • Requirements document • Explicit written User approval or requirements • A list of assigned staff (probably analyst only at this time) • Project Control document
2	High Level Analysis and Design	▪ Research and documentation ▪ Review High Level Analysis and Design document with sponsors ▪ Staff Requirements	• High Level Analysis and Design Document (template available) • Explicit written Sponsor approval of agreed upon alternative (template available) • Explicit written Sponsor approval of agreed upon alternative (template available) • High Level Analysis & Design Summary document • Explicit written Sponsor approval of agreed upon alternative • OIS resources assigned to project by your approving authority • Business resources assigned to project by the Sponsor

3	Detailed Analysis and Design	▪ Document system changes needed to meet User requirements ▪ Document detailed specifications of the changes to the objects defined in 3.1. ▪ Review Detail Design ▪ Revise plan ▪ Implementation Plan	• Resource Requirements (template available) • System Test • Detailed Analysis and Design document (template available) • Detailed Analysis and Design approval • Written approval of revised timeline and scope by Approving Authority (template available) • Preliminary Implementation Plan (template available) • Detailed specifications approval • Revised timeline and scope approval and signoff
4	Construction	▪ Create test scripts ▪ Coding ▪ Unit test ▪ Code review ▪ Update system test plan	• Test scripts • Code • Unit tested code • Unit-level test scripts with unit test results documented • Reviewed code • Compiled, functioning application • Updated system test plan • Test scripts • Compiled, functioning application • Updated system test plan • Preliminary implementation plan
5	Testing	▪ System Testing ▪ Integrated systems testing ▪ User Acceptance ▪ Pilot testing ▪ Finalize implementation plan	• Completed system test • Test scripts with system testing results documented • Completed integrated systems test • Test scripts with integrated system testing results documented • Explicit written Sponsor and User Group approval of system test results (approval template available) • Test scripts with user acceptance testing results documented • Functioning application in pilot environment

			• Finalized implementation plan • Explicit written Sponsor and User Group approval of system test results • Functioning application in pilot environment • Finalized implementation plan
6	Implementation	▪ Execute implementation package ▪ Implementation coordination meeting ▪ Stakeholder notification ▪ Training ▪ Implementation Deployment ▪ Verify implementation	• Completed implementation package • Go/no go decision • Implementation notification • Completed training • Implemented changes or enhancements • Successful technical implementation has been verified • Implemented changes or enhancements
7	Post Implementation	▪ Notify stakeholders ▪ Determine satisfaction ▪ Close the request	• Stakeholders are aware that implementation has occurred. • Written sponsor approval (template available) • Closed request

It is imperative that all software development projects have a comprehensive Project Charter precedent to project initiation. In addition, the processes must adopt a documentation standard including: Context Diagram (CD), Entity Relationships Diagrams (ERD), Data Flow Diagrams (DFD) and Process Maps as appropriate at each stage.

4.7.2 General Development Process Guidelines

To lead and manage system development process a project team will be formed by the MDA that requires a system. This process applies to all application/software development projects including maintenance projects. The following conditions are necessary for a successful development process:

(i) The Project Team and Application Development (PTAD) issue a written statement selecting the development methodology. If there is need to change the application development methodology, the change must also be made in writing and documented.

(ii) The PTAD documents the outputs used in the SDLC processes and methods. The PTAD should document and resolve problems and non-conformances found in the application/software products and tasks by use of a problem resolution process.

(iii) If COTS is being used, the project team must determine that the product satisfies the needs of a particular application development or modification project. The commercial software packages must be compatible with existing GoK IT standards, policies, and guidelines. Software product acquisition procedures must follow the GoK procurement policies, and these products must be reviewed, assessed and tested and reviewed prior to being used. The end-to-end solution must be thoroughly tested as well.

(iv) In the case of a Request for Proposal (RFP) for Contract Application Programming, the PTAD must ensure that a contract programmer adheres to these standards. The end products of completed contract programming services must be reviewed, tested and approved.

(v) The PTAD must support audit(s) and reviews. The results of the audits/reviews must be documented. Upon successful completion of the audits, the PTAD should update and prepare the appropriate deliverables as well as obtain sign-off for the audit.

(vi) To capture and implement security and privacy requirements accordingly, special consideration of the same should be taken throughout the entire project on an ongoing basis. The post-implementation review must reflect this.

4.8 Procurement

Procurement of software shall be done with consultation and coordination of the Head of ICT Unit who shall be responsible for the preparation and issuance of all technical specifications for the software, as well as ensuring that the guidelines stipulated herein are adhered to. MDAs shall use requisition and acceptance forms to ensure that requests for procurement of software are validated by the respective Heads of Department. MDAs shall also ensure that requirements are clearly defined and documented when procuring enterprise software. Where possible, MDAs shall endeavour to use enterprise version of software.

MDAs shall make sure that there is no already existing software application within Government that provides equivalent functions and that can be replicated in the organization before procuring any software to avoid duplication.

All ICT software procured or donated to MDAs shall be received by the Head of ICT Unit who shall ensure proper custody and issuance. All donations shall be required to meet the minimum specifications. Further, all software and assets (new, transferred and/or written off) shall be recorded by the ICT Unit for audit and other managerial purposes.

MDA's shall endeavour to procure and use the latest version of software. Where a previous version of software is to be used, MDA's shall be required to give justifications.

Technical evaluation shall be undertaken to ensure that the software is fit for the purpose it is being acquired for and that it meets the provided specifications. Upon delivery of the software, the ICT Unit shall inspect and ascertain that they meet the laid down specifications. The Head of ICT Unit shall ensure that technical evaluation and inspection reports are prepared respectively.

The Head of ICT Unit shall ensure that an agreement is in place to warrant software support and replacement when required, and that such agreements acquired are enforced.

4.9 Installation of Software

- Software will only be installed by ICT officers in MDAs. Users are not authorized to install any software on computers.

- Software shall only be installed, modified, de-installed or deleted in accordance with agreed change management procedures, and must only be undertaken by ICT Officers in MDAs or authorized IT Partner personnel.

- Users may not give software to any third parties including clients, customers and contractors. Users may use software on networks or on multiple machines only in accordance with applicable licence agreements.

- Manuals, tutorials and other end user materials will be provided to the user where available.

4.10 Maintenance

ICT Units shall keep an inventory of all software in the MDA, and give annual reports on status of utilization, support and adaptability. The software inventory shall be classified according to the following table.

No.	General Classification	Types
1	Operating system	i. Desktop ii. Server iii. Networks
2	Office Productivity	i. Word processors ii. Spreadsheets iii. Presentation iv. Publishers
3	Utilities	i. Backup ii. System Management Software iii. File Management Software iv. Security Software
4	Application Software	i. In house Developed ii. Outsourced Software iii. Commercial Software
5	Web development and Management software	i. Content Management software ii. Web development software iii. Web hosting software
6	Database Software	i. Relational Database Management Systems

		ii. Flat File Based Database Management Systems iii. Hierarchical Database Management Systems iv. Network Database Management Systems v. Object-oriented Database Management Systems
7	Communication Software	i. Email systems ii. Collaboration systems iii. VOIP iv. Teleconferencing v. Mobile Messaging vi. Video conferencing
8	Network Management Software	i. Network monitoring and analyzers ii. Bandwidth management software iii. Network management software

MDAs shall also determine which software have expired licenses for the purposes of upgrade or disposal. Where such systems have proprietary data, that data shall be extracted using suitable mechanisms.

Software media and administration documentation, whether hardcopy or electronic, shall be securely stored in a central repository and copies may be created for backup and disaster recovery purposes as permitted by the license terms and conditions.

Software maintenance shall be done in-house by ICT Units who shall develop a maintenance schedule on upgrading and debugging. Sub-contracting for software maintenance shall be through appropriate justification and approval by the Accounting in consultation with DeG. Due diligence shall be undertaken in retaining such contractors. The Head of ICT Unit shall prepare an annual maintenance report and forward it to the Accounting Officer. Software media shall be tagged with the standard government labeling conventions and appropriately physically secured.

4.11 Disposal

ICT Units shall maintain a record of software media at all times including track of the physical location and status. MDAs wishing to dispose media shall seek the advice of the Head of ICT Unit. Software media that have become obsolete may be disposed of by forwarding to licensed e-waste handlers.

ICT units in MDAs shall regularly evaluate software to determine its relevance to the organization. When application software has expired or reached its end of life it must be uninstalled from the system. For system software patching must be managed until such a time that a new application is installed. Source code and libraries must be safely and securely removed from repositories once obsolete. All software uninstallations shall be documented and retirement of any enterprise applications shall be validated, reported and signed off on.

4.12 Prohibited Software

It is expressly forbidden to possess, distribute, reproduce or use computer programs for reasons such as scanning networks, intercepting information or password capture unless specific authority is obtained or held.

4.13 Software copyright compliance

1. The MDAs will only use a genuine copy of legally acquired software that is configured and used in accordance with the licence terms and conditions as set out by the copyright holder.

2. The making or use of unauthorized or illegal software copies is prohibited in all MDAs. Where possible, controls will be in place within the MDAs to prevent the making or use of unauthorised or illegal software copies. These controls will include effective measures to verify compliance with acquired software licences.

4.14 Software Audits

DeG will periodically conduct audit of software in MDAs, to ensure that they comply with all software licences and the software developed meet the required guidelines.

4.15 Training and Knowledge transfer

MDAs shall ensure that ICT officers mandated to maintain or support software acquired are adequately trained. Where a maintenance contract is in place, MDAs shall ensure that measures are put in place to enforce knowledge transfer to ICT officers by contractors and vendors for continuous support and maintenance of the system once the contract expires.

CHAPTER 5

ICT EQUIPMENT MANAGEMENT GUIDELINES

5.1 Introduction

These ICT equipment management guidelines are based on the prevailing current technology, recognizing the current needs of Government end-users. Guidelines stipulated herein shall apply and be used in the acquisition, support and disposal of all ICT equipment.

The rationale for ICT equipment management guidelines are:

- Ensuring MDAs receive value for money on ICT equipment
- Ensuring compatibility and interoperability both with and across MDAs
- Easy maintenance
- Ensure cost effective use by sharing of ICT equipment where possible.
- Assuring consistency in ICT equipment performance
- Maximize the equipment functionality
- Improve end-user performance and experience
- Guide procurement and disposal

These guidelines shall direct MDAs in their use and management of all ICT equipment not limited to personal computers, desktop workstations, laptops, printers and peripherals devices. However, telecommunications equipment such as routers, are not covered here but in the Network Management Guidelines.

In addition, in line with industry developments it is critical that all equipment especially servers, switches and routers shall support IPv6 and those that do not shall be upgraded.

5.2 Roles and Responsibilities

The Directorate of e-Government (DeG) shall develop and update the minimum specifications, of all categories of equipment on a regular basis, to ensure that prevailing state-of-the-art equipments are acquired for the purpose of enhancing value for money/cost effectiveness, extended useful life, and matching the equipment with the required function. The Heads of ICT Unit shall enforce these standard specifications and give advice where specifications above the minimum are required.

ICT Units shall be charged with the responsibility of installation, upgrading, support and maintenance of the equipment. They shall also sensitize end-users on the proper usage of equipment in their custody.

End-users shall take care of any ICT equipment allocated to them. Any issues arising in the course of usage of the equipment shall be brought to the attention of the ICT Unit. End-users are **prohibited** from carrying out any installation, maintenance or upgrade of any nature.

5.3 Procurement

Procurement of ICT equipment shall be channeled through the Head of ICT Unit who shall be responsible for the preparation and issuance of all technical specifications for the equipment, as well as ensuring that the guidelines stipulated herein are adhered to.

MDAs shall use requisition and acceptance forms to ensure that requests for procurement of ICT equipment are validated by the respective Heads of Department. It is recommended that the Head of ICT Unit be involved in the technical evaluation and inspection processes.

All ICT equipment procured or donated to MDAs shall be received by the Head of ICT Unit who shall ensure proper custody and issuance. All donations shall be required to meet the minimum specifications. Further, all equipments and assets whether new, transferred and/or written off, shall be recorded by the ICT Unit for audit and other asset managerial purposes.

Technical evaluation shall be undertaken to ensure that the equipment is fit for the purpose intended and that it meets the require specifications. Upon delivery of the equipment, the ICT Unit shall inspect and ascertain that they meet the specifications as requisitioned.

The Head of ICT Unit shall ensure that agreements on warranty and guarantees are provided and shall also oversee their administration. The minimum warranty for all ICT equipment shall be one year and three years for servers.

5.4 Maintenance

ICT Units shall keep an inventory of all ICT equipment in the MDA, and give annual reports of equipment status. They shall also undertake surveys to identify obsolte equipment for the purposes of disposal. Where such equipment contain data, that data shall be permanently erased using suitable tmechanisms.

ICT equipment maintenance shall be done in-house by ICT Units where a maintenance function shall ne be established. The unit shall develop a schedule of maintenance for equipment as well as an equipment upgrading plan. Sub-contracting for maintenance shall be through appropriate justification and approval by the Accounting in consultation with DeG. Due diligence shall be undertaken in retaining such contractors. The Head of ICT Unit shall prepare an annual maintenance report and forward it to the Accounting Officer. ICT equipments shall be tagged with the standard government labeling conventions and appropriately physically secured.

5.5 Disposal

ICT Units shall electronically track the physical locations and status of all equipment. MDAs wishing to dispose equipment shall seek the advice of the Head of ICT Unit. ICT equipment identified for disposal but deemed to be still usable may be transferred to other agencies and installed for low-end non-critical use where appropriate. Adherence to the statutes and regulations must always be observed.

When equipment is identified for disposal, all application software should be removed and data permanently erase. The inventory tags shall also be removed and destroyed while updating the inventory system. MDAs may dispose of equipment in either of the following manner: depending on the circumstances and condition of the equipment:

- **Selling:** All ICT equipment no longer of use to MDAs shall be sold wherever possible.
- **Cannibalizing:** ICT equipment that can neither be used in whole nor sold, but have useful components, shall be cannibalized for those components. Proper records shall be kept to indicate where such components are used or stored.
- **Donating:** MDAs shall upon authority from the Accounting Officer donate identified equipment and components, to deserving Government institutions.
- **Trashing:** ICT equipment that cannot be sold and have no useful components, and are not worth donating, shall be trashed. Such equipment shall be forwarded to licensed e-waste handlers.

5.6 Minimum Hardware Specifications

DeG shall endeavor to provide minimum specifications for commonly used ICT equipment, as a measure of ensuring standardization of equipment used across government. In developing minimum hardware specifications, the guidelines put the following criteria into considerations:

- **Total lifecycle:** These specifications are meant to ensure that equipment acquired have useful life of not less than five years.
- **Long-term support:** This addresses the availability of vendor and/or internal support, including parts and labor.
- **Interoperability:** This seeks to facilitate the exchange of information between potentially heterogeneous systems through conformance to open standards.
- **Compatibility**: This addresses the ability of ICT equipment components to effectively and efficiently work together in an integrated system.
- **Scalability**: This is intended to ensure that the acceptable ICT components enhance the ability of the system to support future growth and increased throughput.
- **Availability**: This seeks to maintain a system's operational readiness through robust and/or redundant (e.g. fault tolerance) equipment.
- **Accessibility**: This addresses operational readiness that includes the ability of users and operators to access the system in a timely fashion, to perform its intended functions.
- **Functionality:** This intends to guarantee that operational requirements intended to be performed by ICT systems, can be achieved effectively and efficiently with the equipment specified.
- **Security:** This addresses the need to protect system data and equipment, and the operational environment from loss or compromise. Each workstation connected to the Internet shall have a host antivirus and firewall active at all times.
- **Upgradability:** ICT component installations that need updates shall be updated according to the latest official versions available.

APPENDIX 1

ICT HARDWARE SPECIFICATIONS

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

DESKTOP COMPUTER

ITEM	REQUIREMENT
Processor & Core Logic	Intel Core i3 processor (2.30-GHz, 2 MB L2 cache, 1066-MHz FSB) or Higher
System Memory	Standard 2 GB, Upgradeable to at least 8 GB
Storage Subsystem	At least 250GB 7200 rpm SATA 3.0
Form Factor	Micro Tower
Display/Graphics	17" TFT Flat panel Color LCD, Same brand as CPU 1024x768.
Optical Drives	16X DVD+/-RW
Keyboard and Pointing Device	Enhanced keyboard 2 Button Scroll mouse
Audio	Stereo audio system with 2 speakers
Communication interface	10/100 Mbs Fast Ethernet 56K ITU V.90 data/fax modem, wake-on-ring ready
I/O interface ports	1 x PS/2 compatible keyboard or USB
	1 x PS/2 compatible mouse or USB
	1 x 25 Pin Parallel Port
	Front and rear USB Ports
	1Xrj45 jack for Ethernet
	1 x External VGA Port
Operating System	MS Windows ® 7 down-gradable to XP Professional licensed with CDs
Software	Latest Version, MS Office 2007 licensed with CDs Latest Version of anti-virus with licensed CDs
Power supply	220 – 240 VAC , 50/60 Hz
Warranty	One (1) Year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

LAPTOP COMPUTER

ITEM	REQUIREMENT
Processor & Core Logic	Intel(R) Core(TM) i3-370M Dual Core processor (2.40GHz, 3MB L3 Cache) or higher
System Memory	Standard 2 GB, Upgradeable to at least 4GB
Storage Subsystem	At least 160GB 7200 rpm SATA 3.0
Optical Drives	16X DVD+/-RW
Keyboard and Pointing Device	Enhanced keyboard 2 Button Scroll mouse
Audio	Stereo audio system
Communication interface	10/100 /1000 Mbs Ethernet
I/O interface ports	1 x PS/2 compatible keyboard or USB
	1 x PS/2 compatible mouse or USB
	1Xrj45 jack for Ethernet
	1 x External VGA Port
Operating System	MS Windows ® 7 down-gradable to XP Professional licensed with CDs
Software	Latest Version, MS Office 2007 licensed with CDs Latest Version of anti-virus with licensed CDs
Accessories	Executive leather carry case
Power supply	220 – 240 VAC , 50/60 Hz
Warranty	One (1) Year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

MAC LAPTOP COMPUTER

ITEM	REQUIREMENT
Processor & data bus	2.53GHz Intel Core i5 processor with 3MB shared L3 cache; 1066MHz –data Bus
System Memory	Standard 2GB, Upgradeable to 8 GB DDR3 SDRAM –1066MHz
Storage Subsystem	300GB – serial ATA–5400rpm hard drive, 16X DVD+/-RW
Power System	Power management standard to support standby and Hibernation power saving modes 60Wh battery pack, 4 hours Batter life
Display/Graphics	15.4" TFT Colour LCD, LCD display at 1440 x 900 GDDR3 SDRAM 254MB
Keyboard and Pointing Device	84/85/88 Key, Built-in pointing device, 12 function keys, 4 cursor keys Embedded numeric pad
Audio	PCI 3D audio system, sound card, Built in Microphone 2 external speakers same brand as laptop
Communication interface	Gigabit Ethernet, RJ 45 jack, Wireless-LAN
I/O interface ports	1 x audio –SPDIF Input
	1 X Audio – SPDIF output
	1 x 9 Pin Serial Port
	1 x 25 Pin Parallel Port
	4 x USB Port
	1 x External VGA Port
Operating System	Apple Mac OS X v10.6
Accessories	Carry Case, Mouse
Warranty	One (1) Year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

NOTEBOOK COMPUTERS

ITEM	REQUIREMENTS
Processor and Duo core	At least 2.0 GHz Intel Pentium M L2 Cache or equivalent
System Memory	Standard 2GB SDRAM Upgradeable to 4 GB
Storage	160 GB HDD
	DVD-RW
Power System	Power management standard to support standby and Hibernation power saving modes
	60 Wh battery Pack,
	At least 4 hour Battery life (when unplugged)
Display Graphics	14" TFT Color LCD, 1024 X 768
Keyboard and pointing device	Windows Keyboard
	Built-in pointing device
	12 function keys, 4 cursor keys
Audio	PCI 3D Audio system
Communication interface	10/100/1000 Mbps Ethernet, RJ45 jack, Built-in Wireless connectivity facility, Bluetooth Wireless Technology, Webcam
I/O Interface	4xUSB ports
	1xExternal VGA Port
	1 AC Power Connector
Operating System	MS Windows 7 Professional Installed (Include Licensed CD) ,
Software	MS Office 2007 Professional installed & Licensed (Non OEM) Include Licensed CD
	Include PDF reader & writer ,DVD/CD Burning Software, Media Playing Software
	Most Current Antivirus Solution with current updates
Accessories	Carry Case ,power adapters, external optical mouse
Warranty	1 Year Onsite Repair & Replace
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

TABLET COMPUTER

ITEM	REQUIREMENTS
Notebook Tablet series	Handwriting and voice recognition enabled through MS Windows 7 Professional. Handwriting must be digitized with an industry standard WACOM digitizer
Processor and core Logic	Intel® Core™2 Duo Processor L7500 (2.2GHz, 4MB, 800MHz)
Weight	1.70 kg (3.5 lb) or (4.0 lb inclusive of accessories)
System Memory	Up to 4GB PC2–5300/677MHz (3GB addressable with 32-bit OS)
Storage	160 GB HDD
	External (DVD-ROM/CD-ROM) - RW.
	Data Security with Embedded Security Subsystem (TCG)
	Secure Digital card slot for options that enable storage expansion.
Power System	Power management standard to support standby and Hibernation power saving modes
	Battery life of up to 6.3 hours on 8-cell Li-lon Battery life
Display Graphics	12.1" TFT super-wide Angle with Anti-Reflective/Anti-Glare Protective Coatings Color LCD, 1024 X 768
Keyboard and pointing device	84/85/88 Key
	Built-in pointing device
	12 function keys, 4 cursor keys
	Embedded numeric pad
Audio	PCI 3D Audio system
	Built-in microphone
Communication interface	10/100Mbps Ethernet, RJ45 jack(NIC), RJ-11 Port (Modem), Bluetooth and wireless Technology
I/O Interface	3xUSB ports
	1xExternal VGA Port
	1 AC power
	Docking station with Parallel port, male serial port, vga connector, 2 USB ports, R-J45, R-J11(telecod connector)
Operating System	MS Genuine Windows 7 Professional Installed (Include Licenced CD)
	MS Office 2007 Professional installed & Licensed (Non OEM) Include CD
	Include PDF reader & writer and Media Playing Softwares
	Antivirus Solutions with most current updates.
Accessories	Fingerprint reader,
	At least a 128 MB Graphics Accelerator 900
	Carrying Case, power adapter and external optical mouse
Warranty	1 Year OnSite Repair & Replace
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

WALL MOUNTED LCD PROJECTOR

ITEM	REQUIREMENT
Resolution	XVGA (1024x768) pixel
Display	Poly-Silicon TFTx3 with micro lens army
Brightness	3000 ANSI Lumens
Contrast Ratio	500:1
Video signals	NTSC, PAL,SECAM
Input Signal Format	Video: NTSC, SECAM, SVGA, RGB: VGA, SVGA, And XVGA.
Output Terminal	1xRGB, 1x Audio, Pc control, Screen control, 1xS-video
Audio	2x2.5 Watt Stereo
Aspect Ratio	4:3
Zoom / Focus	Digital zoom
No. of Colours	16.7 million
Lens	Powered Zoom and Focus
Image Size	100cm-700cm-diagonal
Connectivity	802.11b/g wireless
	100/1000 Base-TX
	USB
	PCMCIA
Lamp	270 watt, 1500hours
Accessories	Lens Cap, carry case, Computer VGA cable, product documentation set
Remote control	Wireless remote for projector with pointer, source selection power, resize, mouse functions, volume, preset
Power supply	220-240v, 50/60HZ
Warranty	At least 1Year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

PORTABLE LCD PROJECTOR

ITEM	REQUIREMENT
Display Technology	3LCD
Max number of colors	16.7 Million
Projector Brightness	At least 2500 ANSI Lumens
Resolution	At least 800X600 Pixels
Supported Resolution	Upto SXGA
Contrast Ratio	2000:1
Projection Lamp	170W UHE-E-TORL
Zoom / Focus	Digital zoom
Throw ratio	1.45-1.96:1
Aspect ratio	4:3
Locking Type	Adjustable Tripod stand screen at least (2032mm*1524mm)
Rated power supply	120-240 AC, 5 0/ 60 Hz (Auto voltage)
Accessories	Premium carrying case, Installation CDs & manuals
Warranty	One (1) year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

LASERJET PRINTER

ITEM	REQUIREMENT
Print Quality	1200 x 1200 dpi
Print Speed and throughput	Up to 45ppm black
Print technology	Laser black
Memory	80MB or higher, expandable
Memory slots	2 x100 –pin DDR DIMM
Processor Speed	At least 540Mhz
First page out	Less than 8 sec
Languages	PCL 5e,PCL 6, Postscript 3 emulation
Media Capacity	100 multipurpose tray 500-sheet input trays
	1 manual feeding tray including envelopes, labels, transparencies and special media Output tray up to 300 sheets
Media Sizes	Letter,legal,executive,A4and A3
Media types	Plain paper, envelopes, transparencies, copier, bond (60 to 200 g/m2)
Duplex printing	Automatic (standard)
Connectivity	IEEE-1284 compliant bi-directional parallel port and/or Universal Serial Bus (USB)
	RJ 45 Ethernet port
Hard disk	20Gb
Duty cycle	200,000 per month
Network	Yes (Standard)
Compatibility	Smart switch printer language sensing
	Linux compatible standard
	PCL XL emulation standard
Software	Drivers for windows server 2003/2008/2010, Windows XP/Vista/2007/'7
Warranty	One year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

COLOR LASERJET PRINTER

ITEM	REQUIREMENT
Print speed, black (best quality mode)	31ppm
Print speed, black (normal quality mode)	31 ppm
First page out (black)	As fast as 10 sec
First page out (color)	As fast as 10 sec
Monthly duty cycle	Up to 100,000 pages
Print resolution, black	Up to 600 x 600 dpi
Print resolution, color	Up to 600 x 600 dpi
Ink cartridges	4 (1 each black, cyan, magenta, yellow); all pre-installed
Paper tray(s), minimum	3
Memory	256MB
Duplex Printing	Automatic
Processor speed	At least 533MHz
Print languages, standard	PCL 6, PCL 5c, postscript level 3 emulation
Maximum Input capacity	Up to 1100 sheets
Connectivity	High Speed USB 2.0
	Two enhanced input/output (EIO slots)
	Gigabit Ethernet Print Server
Compatible operating systems	Macintosh, Windows 2000; Windows XP Home; Windows XP Professional; Windows Vista(R); Windows Server 2003 (32/64 bit); Mac OS X v 10.2 or higher; Linux
Software included	Print drivers and installation software on CD-ROM, PCL6, PostScript Level 3 emulation
Warranty	One (1) Year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

PRODUCTION SCANNER

ITEM	REQUIREMENTS
Recommended Daily Volume	Unlimited
Throughput Speeds*	Up to 200 pages per minute/800 images per minute (Throughput speeds may vary depending on your choice of driver, application software, operating system and PC.) *(200 dpi landscape, letter-size document)
Scanning Technology	Dual Tricolor Plus CCD; Grayscale output bit depth is 256 levels (8-bit); Color capture bit depth is 40-bit (10 bits per red, green, blue and black channels); Color output bit depth is 24-bit
Optical resolution	300 dpi
Illumination	Dual Xenon lamps per side, mercury-free
Output resolution	Black and white: 200/240/300/400 dpi; Color/grayscale: 100/150/200/240/300 dpi
Maximum Document Size	305 mm x 863 mm (12 in. x 34 in.)
Minimum Document Size	64 mm x 64 mm (2.5 in. x 2.5 in.)
Paper Thickness and Weight	With standard feeder: 45 g/m² (12 lb) bond to 200 g/m² (110lb) index; With ultra-lightweight feeder: 25 g/m² (7 lb) rice paper to 75 g/m² (20 lb) bond
Feeder	500-sheet
Multi-feed Detection	Multi-feed detection with ultrasonic technology; three ultrasonic sensors that can work together or independently
Connectivity	IEEE-1394 (FireWire) interface, 6-pin connector; IEEE-1394 card and cable included
Interface Support	TWAIN and ISIS Drivers (included); KODAK Capture Software
Color Touch Screen Control	Operator control via color LCD touch screen
Ergonomic Height Adjustment	Integrated height adjustment span of 25 cm (10 in.) for seated or standing operation
Imaging Features	Perfect Page Scanning, iThresholding, autocrop, aggressive crop, deskew, image rotation, electronic color dropout, dual stream scanning, halftone removal, noise removal, zone processing, toggle patch, automatic color detection, automatic orientation
On-board Compression	CCITT Group IV, JPEG or uncompressed output
File Format Outputs	JPEG (for color and grayscale images); TIFF (for black and white images)
Image Address	Multi-level indexing/batching capabilities
Patch Readers	Four permanently mounted patch readers that can work together or independently
Imprinting	Front pre-scan or rear post-scan imprinting; optional hi-res imprinter available
Electrical Requirements	100-130 VAC, 50/60 Hz, 7 A; 200-240 VAC, 50/60 Hz, 3.5 A
Minimum PC Configuration	Pentium 4 2.4 GHz processor with 512 MB RAM
Supported Operating Systems	WINDOWS XP Pro (32bit only) WINDOWS Vista (32 and 64 bit) WINDOWS 7 (32 and 64 bit)
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

DEPARTMENTAL SCANNER

ITEM	REQUIREMENTS
Recommended Daily Volume	Up to 9,000 pages per day
Throughput Speeds*	Up to 45 pages per minute/90 images per minute *(200 dpi, landscape, letter size, black and white/grayscale/color)
Scanning Technology	dual CCD Grayscale output bit depth is 256 levels (8-bit) Color capture bit depth is 48 bits (16 x 3) Color output bit depth is 24 bits (8 x 3)
Output resolution	75, 100, 150, 200, 240, 300, 400, 600 and 1200 dpi
Maximum Document Size	297 mm x 863 mm (11.7 in. x 34 in.)
Minimum Document Size	64 mm x 89 mm (2.5 in. x 3.5 in.)
Paper Thickness and Weight	34–413 g/m² (9–110 lb.) paper
Feeder	Up to 150 sheets of 60 g/m² (16 lb.) paper
Multi-feed Detection	With ultrasonic technology
Connectivity	USB 2.0
Bundled Software	TWAIN, ISIS, SANE and Windows Imaging Architecture Drivers, KODAK Capture Desktop Software and Smart Touch
Imaging Features	Perfect Page Scanning; Thresholding; adaptive threshold processing; deskew; autocrop; relative cropping; aggressive cropping; electronic color dropout; dual stream scanning; interactive color, brightness and contrast adjustment; automatic orientation, automatic color detection, background color smoothing
File Format Outputs	Single and multi-page TIFF, JPEG, RTF, PDF, searchable PDF
Accessories	KODAK Imaging Guide Wiper Accessory Optional A4 black imaging background accessory
Electrical Requirements	100-240 V (International); 50/60 Hz; universal power supply included
Recommended PC Configuration	For documents up to 356 mm (14 in.) long at 400 dpi: Pentium 4, 3.2 GHz processor, 512 MB RAM; For documents up to 660 mm (26 in.) long at 400 dpi: Pentium 4, 3.2 GHz processor, 1 GB RAM; For longer documents/higher resolutions: Pentium 4, 3.2 GHz processor, 3 GB RAM
Supported Operating Systems	Windows 7 (32-bit and 64-bit) Windows XP SP2 (32-bit) Windows XP x64 Edition SP2 Windows 2000 Professional SP4 Windows Vista SP1 (32-bit and 64-bit) Windows 2003 Server x64 Edition LINUX Ubuntu 6.06, Fedora 8, and SUSE 10.1
Consumables Available	Feed module, separation module, feed rollers, roller cleaning pads, Staticide Wipes, image guides, pre-separation pad
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

WORKGROUP SCANNER

ITEM	REQUIREMENTS
Recommended Daily Volume	Up to 3,000 pages per day
Scanning Technology	Single CCD; i1220 Plus: Dual CCD; Grayscale output bit depth is 256 levels (8 bits); Color capture bit depth is 48 bits (16 x 3); Color output bit depth is 24 bits (8 x 3)
Throughput Speeds (portrait, letter size)	Bitonal/grayscale: Up to 45 pages per minute at 200 dpi Color: Up to 30 pages per minute at 200 dpi and 300 dpi (Throughput speeds may vary depending on your choice of driver, application software, operating system and PC.)
Optical resolution	600 dpi (1200 dpi A4 flatbed accessory)
Illumination	Dual fluorescent (cold cathode)
Output resolution	75, 100, 150, 200, 240, 300, 400, 600 and 1200 dpi
Max./Min. Document Size	215 mm x 863 mm (8.5 in. x 34 in.)/50 mm x 63.5 mm (2 in. x 2.5 in.)
Paper Thickness and Weight	34-413 g/m² (9-110 lb.) paper; ID card thickness: up to 1.25 mm (0.05 in.)
Feeder	Up to 75 sheets of 75 g/m² (20 lb.) paper Handles small documents, such as ID cards, embossed cards and insurance cards
Multi-feed Detection	With ultrasonic technology
Connectivity	USB 2.0 (cable included)
Bundled Software	TWAIN, ISIS, WIA Drivers; KODAK Capture Desktop Software, Smart Touch; Nuance ScanSoft PaperPort and OmniPage.
Imaging Features	Perfect Page Scanning; iThresholding; adaptive threshold processing; deskew; autocrop; relative cropping; aggressive cropping; electronic color dropout; dual stream scanning; interactive color, brightness and contrast adjustment; automatic orientation; automatic color detection; background color smoothing; image edge fill; image merge; content based blank page detection; streak filtering; image hole fill; sharpness filter
File Format Outputs	Single and multi-page TIFF, JPEG, RTF, BMP, PDF, searchable PDF
Recommended PC Configuration	For documents up to 660 mm (26 in.) long at 400 dpi: Intel Core2, 2 GHz Duo Processor or equivalent, 2 GB RAM. For longer documents/higher resolutions: Intel Core2, 2 GHz Duo Processor or equivalent, 4 GB RAM. Note: for optimal performance when using a PC running the Windows 7 operating system, at least 3 GB RAM is recommended.
Supported Operating Systems	Windows XP SP2 and SP3 (32-bit), Windows XP x64 edition SP2, Windows Vista SP1 (32-bit and 64-bit), Windows 7 (32-bit and 64-bit), Windows 2003 Server and 2008 Server x64 Editions, Linux Ubuntu 8.04, Fedora 9, SUSE 11
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

SMALL OFFICE PHOTOCOPIER

ITEM	REQUIREMENTS
Copying technology	Laser
Duplex copying	Two-sided copying Automatic
Input: Output support	1-1, 1-2, 2-1, 2-2
Copying Speed	20cpm
Copy Resolution	600 x 600 dpi
Minimum Memory / RAM Installed	128 MB
Communication Mode	Duplex
Interfaces	USB 2.0 Parallel Port IEEE 1284,(USB cable included);
Display/ Operation	Touch screen panel
Trays	3 paper trays including the bypass tray; Automatic Document Feeder
Media Type	Papers, envelops, transparencies
Document Feeder Capacity	50 sheets
Standard Tray	250 sheets
Optional Tray	250 sheets
Bypass Tray	100 sheets
Output Tray	250 sheets facedown
Auto Tray Switching	Capable
Media Sizes	Document glass and maximum paper size is legal (8.5 x 14 inches);
Monthly Duty Cycle	Maximum 20,000 pages per month.
Power	220-240 VAC 50/60 Hz
Power Saver Mode	35 watts
Warm up time	30 Seconds max
First copy out time	8 seconds or less
Toner type	Customer replaceable
Toner Control method	Automatic Toner Density monitoring
Finishing options	Multiposition stapling, fit to new paper size, booklet creation
Document scanner	ADF (full duplex)
Zoom range	25-400% in 1% increments
Other features	Secure print, Delay print, Watermark, Power save mode
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

MEDIUM OFFICE PHOTOCOPIER

ITEM	REQUIREMENTS
Copying / Print technology	Laser
Duplex copying/printing	Two-sided copying Automatic
Input: Output support	1-1, 1-2, 2-1, 2-2.
Copying Speed	30 cpm
Multiple copying	Up to 999 copies
Copy Resolution	up to 1200 x 1200dpi
Memory	512MB expandable to 1024
Hard drive	40GB
Communication Mode	Duplex
Interfaces	USB 2.0 Parallel Port IEEE 1284,(USB cable included);
Trays	3 paper trays including the bypass tray
Media Feed	Include Duplex unit, Automatic media feeder;
Document Feeder Capacity	75 sheets
Output Tray	250 Sheets
Standard Tray	500 Sheets
Optional paper supply	500 Sheets
By pass Tray	100 Sheets
Auto Tray Switching	Capable
Media Sizes	Document glass and maximum paper size is legal (11 x 17 inches); Automatic media feed.
Media type	Paper, Envelopes, labels, cards
Monthly Duty cycle	Maximum 100,000 ppm.
Display/ Operation	Touch screen panel
Power	220-240 VAC 50/60 Hz; consumption 1340 w (max)
Power Saver Mode	35 watts
Warm up time	30 Seconds max
First copy out time	5 seconds or less
Toner Control method	Automatic Toner Density monitoring
Toner	Customer Replaceable
Finishing options	Multi-position stapling, fit to new paper size, Hole punch, booklet creation
Document scanner	ADF (full duplex)
Output capacity	250 Sheet face down
Zoom range	25-400% in 1% step
Other features	Secure print, Delay print, Watermark
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

LARGE OFFICE PHOTOCOPIER

ITEM	REQUIREMENTS
Copying / Print technology	Laser
Duplex copying/printing	Two-sided copying Automatic (standard)
Copying Speed	45cpm
Copy Resolution	Up to 2400 x 600 dpi /4800 x 600 dpi interpolated output
Memory / RAM Installed (Min)	1GB
Hard drive Capacity	60GB
Communication Mode	Duplex
Interfaces	USB 2.0 Parallel Port IEEE 1284,(USB cable included);
Trays	3 paper trays including the bypass tray.
Multiple Copying	Up to 9999 copies
Media Feed	Include Duplex Automatic media feed tray;
Input: output support	1-1, 1-2, 2-1, 2-2.
Document Feeder Capacity	100 sheets
Output Tray Capacity	500 Sheets
Standard Tray	550 sheets
Optional paper supply	550 Sheets
Bypass Tray	100 sheets
Auto Tray Switching	Capable
Media Sizes	Document glass and maximum paper size is legal (11x 17 inches); Automatic media feed
Media type	Paper, Envelopes, labels, cards
Display /Operations	Touch screen
Monthly Duty Cycle	Maximum 200,000 pages per month.
Power	220-240 VAC 50/60 Hz
Power Saver Mode	35 watts
Warm up time	30 Seconds max
First copy out time	4 seconds or less
Toner Control method	Automatic Toner Density monitoring
Original	Maximum A3
Finishing options	Multi-position stapling, fit to new paper size, hole punch, booklet creation
Document scanner	ADF (full duplex)
Output capacity	250 Sheet face down
Zoom range	25-400% in 1% step
Other features	Secure print, Delay print, Watermark
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

DSLR DIGITAL CAMERA

ITEM	REQUIREMENTS
Resolution	14.1 Megapixels
sensor type	CMOS
Image Stabilization	Standard
Image Resolution	4320 x 3240
Minimum Shutter speed	60 sec
Minimum continuous shooting speed	3.5 frames per second
Video capture	1280 x 720; 640 x 480 ; 320 x 240
Maximum Frame Rate	30 fps
Digital Video Format	MOV, AVI, MPEG-4,MJPEG, H.264
Still image format	JPEG, RAW,RAW+JPEG
Lens type	Lens mountable
Minimum Lens	18-55mm
optical zoom	10X
Minimum Field of view	1.5
View Finder	LCD
Display resolution	920,000
Light Sensitivity	6400 ISO
Expandable Memory Type:	MS Duo / MS PRO Duo / SD / SDHC/SDXC/MMC
Exposure Modes	Programmable, automatic
Battery:	Li-ion rechargeable battery
Power Device	Battery charger external
Connector type	USB, Composite video/audio
Battery Life	300 shots
Face detection	Standard
Shooting modes	auto, portrait, landscape, night, close-up, snapshot, flash off, indoor , low light, movie
Self – Timer	2 Sec/10 Sec
Flash type	Auto
Flash Mode	Flash On/off, red eye reducer, auto
Sound	Built in Microphone and speakers
Accessories	Rechargeable Li-ion Battery, Battery Charger, Remote Control, USB Cable, Audio/Video Cable, case and strap
Focus Mode	Automatic, Manual
White balance	Custom, automatic, presets
Firmware	User upgradable
Software	Windows XP/ Windows Vista/ Windows 7/Mac/ Linux compatible image viewing software
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

COMPACT DIGITAL CAMERA

ITEM	REQUIREMENTS
Resolution	14.1 Megapixels
sensor type	CCD
Pixel Density	24 MP/cm²
Still image format	JPEG
Image Stabilization	Optical/lens
Image Resolution	4320 x 3240
Minimum Shutter speed	60 sec
Video capture	1280 x 720; 640 x 480 ; 320 x 240
Maximum Frame Rate	30 fps
Digital Video Format	MOV, AVI, MPEG-4,MJPEG
Optical zoom	10 x
Minimum wide angle zoom	25mm
View Finder	LCD
Display Resolution	460,000
Light Sensitivity	3200 ISO
Built in Memory	40MB
Expandable Memory Type:	MS Duo / MS PRO Duo / SD / SDHC/SDXC/MMC
Exposure Modes	Programmable, automatic
Battery:	Li-ion rechargeable battery
Power Device	Battery charger external
Connector type	USB, Composite video/audio
Battery Life	300 shots
Operating system compatibility	Linux, Windows XP, Windows Visa, Windows 7
Face detection	Standard
Shooting modes	auto, portrait, night snapshot, indoor and low light,
Self – Timer	2 Sec/10 Sec
Flash type	Built-in;
Flash Mode	Flash On/off, red eye reducer, auto
Sound	Microphone and speakers built in
Accessories	Rechargeable Li-ion Battery, Battery Charger, Remote Control, USB Cable, Audio/Video Cable, case and strap
Lens type	Built in
White balance	Custom, automatic, presets
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

PROFESSIONAL DIGITAL CAMCORDER

ITEM	REQUIREMENTS
Image Sensor	CMOS/ 3M0S
Image Sensor size	1/4 in
Minimum Filter Diameter	40 mm
Total minimum pixels	8 MP
Minimum Digital Zoom	200 X
Optical Zoom	10 X
Min Focal Length	40 mm (35 mm equivalent)
Minimum Shutter Speed	1/30 (Auto slow shutter On); 1/60(Auto slow shutter Off)
Image Stabilization	Optical
Audio Support	5.1 Surround Sound, AC-3 (2 channels)
Video Capture Format	HDV ,MPEG-2, MPEG-4, AVC/H.264 (HD Compliant)
Maximum Video Capture Resolution	1440 x 1080
Display type	LCD
Display resolution	200,000 pixels
Video Broadcast Standard	NTSC
Video signal	1080/60i
Recording Media	Memory Stick Duo, Memory Stick PRO Duo, Sony Memory Stick Image Capture (SD/SDHC/SDXC), High Definition Mini DV (recommended) ,MiniDV cassette
Flash	Accessory Shoe, Red-Eye Reduction
Still Camera resolution	10MP
Image Format	JPEG
White Balance	Auto, outdoor, indoor, daylight, sunny, shade, cloudy, manual
Exposure Settings	Auto Exposure, Manual Exposure
Internal Memory type	Hard drive/Flash Memory
Minimum Internal Memory	32 GB
Included Components	AC Adapter, Battery, Battery Recharger, Cables - A/V (RCA Composite), Cables - Component Video, Cables - USB, Docking / Cradle Stand, Remote, software CD/DVD Rom, Carrying case
Interface Connection	SD output, HD output , headphones, A/V Output, Component Video, HDMI, LANC Terminal, Microphone, Proprietary, S-Video, USB2.0 - Universal Serial Bus
Additional Features	Backlight Compensation, Built-in Light, Built-in Speaker, Fader Function, PictBridge Support, Touch Screen, Viewfinder Power
Focus Features	Auto Focus, Face Recognition Auto Focus, Manual Focus, Spot Focus
Power requirement	7.2 V(Battery)
Power Source	AC Adaptor, Lithium-Ion Battery
Focus	Auto/Manual
Iris	Auto/Manual
Warranty	1 Year Limited Warranty
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

STANDARD USER DIGITAL CAMCORDER

ITEM	REQUIREMENTS
Image Sensor	CMOS
Image sensor size	1/8 in
Minimum Filter Diameter	40 mm
Total minimum pixels	10 MP
Minimum Digital Zoom	100 X
Optical Zoom	12 X
Min Focal Length	40 mm (35 mm equivalent)
Minimum Shutter Speed	1/30 (Auto slow shutter On); 1/60(Auto slow shutter Off)
Image Stabilization	Optical
Audio Support	Stereo
Video Capture Format	MPEG-2, H.264/AVC
Maximum Video Capture Resolution	1920 x 1080
Display type	LCD
Display resolution	200,000 pixels
Video Broadcast Standard	NTSC
Recording Media	Memory Stick Duo, Memory Stick PRO Duo, Sony Memory Stick Image Capture (SD/SDHC/SDXC), ,MiniDV cassette
Flash	Accessory Shoe, Red-Eye Reduction
Still Camera resolution	10MP
Still Image Format	JPEG
White Balance	Auto,outdoor, indoor, daylight, sunny, shade, cloudy, manual
Exposure Settings	Auto Exposure, Manual Exposure
Internal Memory type	Hard drive/Flash Memory
Minimum Internal Memory	32 GB
Included Components	AC Adapter, Battery, Battery Recharger, Cables - A/V (RCA Composite), Cables - Component Video, Cables - USB, Docking / Cradle Stand, Remote, software CD/DVD Rom, Carrying case
Interface Connection	A/V Output, Component Video, LANC Terminal, Microphone, Proprietary, S-Video, USB - Universal Serial Bus 2.0
Additional Features	Backlight Compensation, Built-in Light, Built-in Speaker, Fader Function, PictBridge Support, Touch Screen, Viewfinder Power
Focus Features	Auto Focus, Face Recognition Auto Focus, Manual Focus, Spot Focus
Power Source	AC Adaptor DC Input, Lithium-Ion Battery
Focus	Auto/Manual
Iris	Auto/Manual
Warranty	1 Year Limited Warranty
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

STANDARD USER DIGITAL DVD CAMCORDER

ITEM	REQUIREMENTS
Image Sensor	CMOS/CCD
Image sensor size	1/6 in
Minimum Filter Diameter	30 mm
Total minimum pixels	10 MP
Minimum Digital Zoom	100 X
Optical Zoom	12 X
Min Focal Length	40 mm (35 mm equivalent)
Minimum Shutter Speed	1/30 (Auto slow shutter On); 1/60(Auto slow shutter Off)
Image Stabilization	Optical
Audio Support	Stereo
Video Capture Format	MPEG-2, H.264/AVC
Maximum Video Capture Resolution	1920 x 1080
Display type	LCD
Display resolution	123,000 pixels
Video Broadcast Standard	NTSC
Recording Media	DVD/ Flash Media
DVD Type	DVD-R/-RW/-R DL
Flash	Accessory Shoe, Red-Eye Reduction
Still Camera resolution	10MP
Still Image Format	JPEG
White Balance	Auto, outdoor, indoor, daylight, sunny, shade, cloudy, manual
Exposure Settings	Auto Exposure, Manual Exposure
Internal Memory type	Flash Memory
Included Components	AC Adapter, Battery, Battery Recharger, Cables - A/V (RCA Composite), Cables - Component Video, Cables - USB, Docking / Cradle Stand, Remote, software CD/DVD Rom, Carrying case
Interface Connection	A/V Output, Component Video, LANC Terminal, Microphone, Proprietary, S-Video, USB - Universal Serial Bus 2.0
Additional Features	Backlight Compensation, Built-in Light, Built-in Speaker, Fader Function, PictBridge Support, Touch Screen, Viewfinder Power
Focus Features	Auto Focus, Face Recognition Auto Focus, Manual Focus, Spot Focus
Power Source	AC Adaptor DC Input, Lithium-Ion Battery
Focus	Auto/Manual
Iris	Auto/Manual
Warranty	1 Year Limited Warranty
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

DISK DUPLICATOR

ITEM	REQUIREMENTS
Operating type	Stand alone
Max Writing speed	DVD-R: 24X DVD-RW: 8X DVD-R DL: 10X DVD+R: 24X DVD+RW: 8X DVD+R DL 10X CD-R: 52X CD-RW: 52X
Supporting Discs	DVD-ROM DVD-R DVD-Video DVD-RW DVD+R DVD+RW CD-ROM CD-R CD-Audio Disc CD-RW Multi-session Photo CD CD-I Video CD CD-ROM XA & CD Extra (CD Plus), Blu Ray
Supported Recording Discs	12cm 4.7GB DVD-R/RW 12cm 4.7GB DVD+R/RW 12cm 8.5GB DVD+R DL 12cm 8.5GB DVD-R DL 12cm 80min/700MB CD-R 12cm 74min/650MB CD-RW 8cm 1.47GB mini DVD-R 8cm 24min/210MB mini CD-R 8cm 50MB Business Card CD-R, Blu-ray
Display	LCD
Hard drive	250GB
Hard drive partitioning	Continuous
Buffer Memory	128MB
Connectivity	USB 2.0 and Network connectivity
Firmware upgradeable	Yes
Security	User account management
DVD format conversion	Convert media between DVD+R/RW and DVD-R/RW automatically
Auto counter	Yes
Labeling	Laser labeling technology
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

DIGITAL VIDEO CAMERA

ITEM	REQUIREMENTS
Optical sensor size	1/3 in
Optical sensor type	CMOS
Min illumination	7 lux
Image stabilizer	optical
Min shutter speed	1/4 sec
Shooting modes	Digital photo mode
White balance	Custom, Presets, Automatic
White balance presets	Auto, Indoor, Outdoor, Manual
Lens aperture	F/1.8-2.1
Optical zoom	12 x
Lens system type	Zoom lens
Min focal length	5.1 mm
Auto focus	TTL contrast detection
Filter size	37 mm
Manual focus	Manual, Automatic
Zoom adjustment	Manual, Motorized drive
Media type	Mini DV (HDV) PAL
Image storage	JPEG 1920 x 1440, JPEG 1440 x 1080, JPEG 1920 x 1080, JPEG 640 x 480
Flash memory	16 MB – Memory Stick Duo
Recording speed	SP
Display type	LCD display – TFT active matrix
Display form factor	Rotating
Display resolution	123,200 pixels
Audio input type	Microphone
Microphone type	Built-in
Microphone operation mode	Stereo
Connections	1 x Component video output, 1 x Composite video/audio output, 1 x S-Video output, 1 x Headphones, 1 x Audio input, 1 x Control-L (LANC), 1 x USB, 1 x DC power input
Cables included	A/V cable, Component video cable, USB cable
Video input features	Built-in speaker, Histogram display, Backlight compensation, RGB primary color filter, Analog to digital conversion with pass through Remote control Remote control – Infrared
Included accessories	Lens cap, Lens hood, Camcorder shoulder strap, Memory Stick Duo adapter,
Power	External power adaptor 240v, Lithium rechargeable battery pack, charger
Warranty	1 Year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

VIDEO RECORDING PRESENTER WITH LASER POINTER

ITEM	SPECIFICATIONS
Technical features	4-in-1 Product - Product functions as a • PowerPoint presenter • with laser pointer, • integrated voice recorder and • SD memory card reader
Storage	Built-in SD memory card reader and SD Card Storage - Allows recording of presentations, meetings or notes and save to a SD card in .wav format;
Wireless	2.4GHz wireless technology that provides up to a 50-foot (15m) working range for full control of the presentation from anywhere in the room
Stow-n-go® receiver	USB receiver that can be stored conveniently inside presenter for easier storage and travel
Carrying case	Carrying case with extra storage compartment for 2 spare AAA batteries
Led status indicators	SD card memory full, low battery power and laser beam currently in use Indicator lights to notify user of any status changes, so there are no unexpected surprises during an important presentation
System requirements/compatibility	Windows 2000/XP/Vista, USB port,SD memory card
Communication interface	USB Port
Convenience	Easily record any presentation questions with the click of a button
Weight	55 g
Battery	2 AAA batteries and 2 spare AAA batteries
Functions on the presenter	Scroll wheel provides for navigation through presentations; Other buttons include: On/off, Next/previous page, dark screen/resume, application switch, slideshow/ESC and volume control
Warranty	2 years
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

WIRELESS INTERNET MODEM

ITEM	SPECIFICATIONS
Main features	• Micro SD Memory Slot, so can act as a Memory stick. (up to 4GB) • Able to add external Antenna incase signal not enough strong. • Smaller and more compact. • Stable and Reliable. • Compatible with Windows 2000, XP & Vista operating systems and MacOS. • Zero CD Technology: No CD Requires, Auto plug and play. Simple and easy.
Technical standard	HSDPA/UMTS: 3GPP R99, R5 GSM/GPRS/EDGE: 3GPP R99
Operating frequency	HSDPA/UMTS 2100MHz GSM/GPRS/EDGE 850/900/1800/1900MHz
Support speed	Maximum download speed : 3600 kbps Maximum upload speed : 384 kbps
External interface	Mini USB interface: supporting USB 2.0 Full Speed Antenna: Internal antenna External Antenna Slot: Able add external antenna. With Extra Micro SD Memory Slot (up to 4GB). SIM/USIM card: standard 6 PIN SIM card interface
Dimensions	70.1 mm (D) x 25.7 mm (W) x 11.6 mm (H)
Usb	Auto plug and play
Weight	< 50g
Led indicator	- Green Light You are connected to the GPRS/EDGE network (fast) - Blue Light You are connected to the 3G network (faster) - Cyan Light You are connected to the HSDPA or Turbo network (fastest)
Warranty	One Year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

DIGITAL LCD DISPLAY PANEL

ITEM	SPECIFICATIONS
Picture/display	
Aspect ratio	16:9
Size	Between 47"
Brightness	500 CD/M2
	Total Input-Line: 4 ,Total Input-Terminal: 4
Contrast ratio	1600: 1 Dynamic Contrast Ratio,
Display screen	LCD WXGA Active Matrix TFT
Screen enhancement	Anti Reflection Coated Screen
Viewing angle	Horizontal: 178°, Vertical: 178° Degrees
Audio power output	14W Total (7Wx2 Digital AMP)
Inputs and Outputs Specifications	Analog Audio Input(s) -Pinjack (x2), Analog Audio Output(s)-Pinjack (x2), Composite Video Output(s) - BNC (x1) Loop Through Dual Option Slot-1.8 Slot, Ethernet Connection(s), HD Component Video Input(s) RGB/COMPONENT IN: HD D-sub 15-pin female (x1) HD Component Video Output(s) RGB/COMPONENT Out: HD D-sub 15-pin female (x1) HDMI™ Connection(s) Available through Option Card BKM-FW15 PC Audio Input(s), RS232 Control- D-sub 9-pin (x1) S-Video Input(s) Mini DIN 4-pin (x1): when S-Video is used, Composite Video is inactive Video In (BNC) (x1): when Video is used, S-Video is inactive
Video Specifications Format(s) Supported	NTSC/PAL/PAL-M/PAL-N/NTSC4.43/PAL60 Viewing Angle
	Display Technology 8 ms Picture Mode Custom, Vivid, Standard, Conference, DICOM
Display RESPONSE TIME	8MS
Panel resolution	1920 x 1080 Display Resolution
Sound	Virtual Surround sound
	Stereo sound Output
Remote Control	LAN / RS232 Available
Digital Inputs Specifications	DVI-D, HDSDI (SMPTE 292M) , No (Available through Option Card BKM-FW16)
Power Specifications	Internal Power Supply Yes Power Consumption (in Operation) Approx 320W Power Requirements AC 100-240V, 50/60Hz
HDMI™ Technology	No (Available through Option Card BKM-FW15)
Multiple Language Display	English, French, Spanish, Italian, German, Japanese, Dutch, Swedish, Russian,

	Chinese
On-Screen Display	Yes
Picture and Picture	Yes
	VGA in SUB 15 HD
Convenience Specifications	Cable Management System, Wall/Arm Mount
Mount Design	Landscape, Portrait Auto sensing Logo illumination
Remote Control	Multi-Function Remote
Operating Conditions Specifications	Color Temperature Control -Cool, Neutral, Warm
	Colors -1.06 Billion Colors
	Operating Humidity -20% to 90%, non condensing
	Operating Temperature -32° to 95°F (0° to 35°C)
	Screen Treatment -Anti-Glare, Anti-Reflective
PC Connection	PC : Computer display with support for resolutions up to 1920 x 1080 through HDMI and VGA
SPEAKERS	Mounted speakers with sound audio processor, making theater-quality audio
Warranty	3 years parts, 3 years labor, 1 year panel
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

MULTIPURPOSE PHOTOCOPIER (4 in one)

ITEM	REQUIREMENTS
Printing specifications	
Functions	
All-in-one functions	Print, copy, Scan and Fax
Multitasking capability	Yes
Print quality technology	
Print technology	Laserjet
Print speed, black (normal quality mode)	Up to 40 ppm
Print speed, color (normal quality mode)	Up to 40 ppm
First page out (black)	As fast as 11.5 sec
First page out (color)	As fast as 11.5 sec
Monthly duty cycle	Up to 200,000 pages
Recommended monthly print volume	8,000 to 17,000 pages
Print resolution, black	Up to 1200 x 600 dpi
Print resolution, color	Up to 1200 x 600 dpi
Memory	512 MB
Processor speed	835 MHz
Paper handling	
Paper handling optional, input	1 x 500 Feeder Stand, 3 x 500 feeder stand-one or the other of these should be present with each unit.
Paper handling optional, output	Tray 1 and a Cassette Tray 2 and 3 (Tray 1 holds 100 sheets, Tray 2 and 3 holds 500 sheets each) F Bundle includes and additional 2 x 500 sheet input trays (trays 4 and 5)
Paper handling standard, output	500-sheet face down output bin
Envelope capacity	Up to 10 envelopes
Duplex printing	Automatic
Document finishing	Sheetfeed simplex or duplexed face down to standard output bin; Optional devices handle Stacking, Stapling and Booklet making
Media sizes, standard	Multipurpose tray 1: letter, letter-R, legal, executive, statement, 8.5 x 13 in, 11 x 17 in, 12 x 18 in, index cards (4 x 6, 5 x 8), envelopes (No. 9, 10, Monarch); Input tray 2: letter, letter-R, legal, executive, 8.5 x 13 in, 11 x 17 in; Input trays 3, 4, and 5: letter, letter-R, legal, executive, 8.5 x 13 in, 11 x 17 in, 12 x 18 in
Media sizes, custom	Multipurpose tray 1: 4 x 5.5 to 12.6 x 18 in; Tray 2: 5.8 x 8.3 to 11.7 x 17 in; Trays 3, 4, 5:: 5.8 x 8.3 to 12.6 x 18 in
Media types	Paper (bond, recycled, glossy, mid-weight, heavy, heavy glossy, extra heavy, extra heavy glossy, rough, tough), transparencies, labels, envelopes, cardstock, user-defined
Scanner specifications	
Scanner type	Flatbed, ADF
Scan resolution, optical	Up to 600 dpi

Scan size, maximum (flatbed)	11.7 x 17 In
Scan size, maximum (ADF)	11.7 x 17 In
Scan speed (default)	Up to 40 ppm (mono letter simplex); up to 38 ppm (mono A4 simplex); up to 41 ppm (mono A3 simplex) up to 16 ppm (mono letter duplex); up to 15 ppm (mono A4 duplex); up to 16 ppm (mono A3 duplex)
Scanner features	Yes
Automatic paper sensor	Yes
Supported file formats	PDF, JPEG, TIFF, or MTIFF
Copier specifications	
Copy resolution, black	Up to 600 x 600 dpi
Copy resolution, color	Up to 600 x 600 dpi
Copy reduce/enlarge settings	25 to 400%
Maximum number of copies	Up to 999 copies
Fax specifications	
Faxing	Yes
Fax transmission speed (seconds per page)	13 sec per page
Fax resolution, black (dots per inch)	Up to 300 x 300 dpi (Recv can support 400x400)
Speed dials, maximum number	100 speed dials and 100 numbers per speed dial.
Auto redial	Yes
Fax delayed sending	No
Fax broadcast	100 Locations
Junk fax barrier	Up to Blocked 20 fax numbers
Polling	No
Remote retrieval	No
Fax forwarding	Yes
Warranty	I year
Connectivity	
Connectivity, standard	1 Hi-Speed USB 2.0, 1 built-in wired Ethernet, 1 PictBridge, 1 built-in wireless 802.11b/g
Connectivity, optional	HP bt300 Bluetooth Wireless Printer Adaptor Q3395A
Macintosh compatible	Yes
Print drivers, standard	HP PCL 3 GUI
Compatible operating systems	
Microsoft Windows 7, Windows Vista, Windows XP Home, Windows XP Professional, Windows Server 2003, Windows 2000, Mac OS X v10.2.8, 10.3, 10.4, 10.5, 10.6, Linux	
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

EXTERNAL HARDDISK

ITEM	REQUIREMENTS
Capacity	320 GB
Hard Disk Spindle Speed	7200 rpm
Cache	2 MB
Hard disk Interface	FireWire 800, FireWire 400 and USB 2.0
Data Transfer Rate	480 MB/s
Seek time	14 ms
Compatible operating systems	Windows XP, Windows Vista, Windows 7 and Mac OS 9.x / 10.1 or higher
Power Source	USB bus and FireWire bus
Power Requirements	100 - 240 VAC
Warranty	1 year
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

FLASH DISK

ITEM	REQUIREMENTS
Capacity	2 GB
Rotational Speed	4200 rpm
Cache	2 MB
Interface	ATA 100, Zer Insertin Frce (ZIF) cnnectr / USB 2.0
Max. External Transfer Rate	100 MB/s
SEEK TIME	
Track t Track	3 ms
Average	15 ms
Maximum	26 ms
SHCK	
perating	500G @ 2ms
Nn-perating	1500G @ 1ms
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

INTERNAL SERVER HARDDISK

ITEM	REQUIREMENTS
Capacity	146 GB 10K rpm upgradable to 1.75TB
Maximum Raw Storage	584 GB 10K rpm
Classification	Serve V890 Suns Solaris
Host interface	160 MB SCSI LVD
Hard Disk Drives	160 MB SCSI 3.5 inch low profile
Supported Drives	73 GB 10K rpm; 146 GB 10K rpm
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

STANDBY UPS

ITEM	REQUIREMENTS
Power provided	At least 650 VA
Input Voltage Swing	AC 196 - 280 V
Output voltage Range	AC 230 V
Localization	220 - 240V / 50Hz
Output Frequency	50 - 60HZ auto-sensing
Design	automatic voltage regulaton
	Mains Isolation
	User replaceable batteries
	Static-Automatic bypass
	Run time (full load) 2,4 min
	Maintenance bypass incase of servicing
Battery Module	Minimum 16 minutes backup time on 50% rated outout
	Minimum 5 minutes backup time on100% rated outout
	Minimum 3 year lifetime
	Type (Sealed lead-acid preferred)
	Automatic periodic battery tests
	Short recharge time (Maximum 5 hours for 100% runtime)
	Protection against excessive/damaging discharge
Protection	Output Overload
	Input/Output short-circuit
Communication Interface	Serial port communications support
Warranty	1 Year OnSite Repair & Replace
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

ONLINE/SMART UPS

ITEM	REQUIREMENTS
Product Description	850VA UPS
Power	850Va / 500W
Input Voltage range	165-275 Vac
Frequency	50 Hz
Charging Time	12 hours (90%)
Battery type (Ah)	Air-tight, maintenance-free, lead battery with anti-leak seal
Autonomy	1.5 min (full load) - 7 min (medium load)
Output voltage (Single Phrase)	230Vac + 10% - 15%50Hz 5% in-line
Power (kVA/KW)	850 Va/500 W
Output number	Back: 2 IEC sockets + 2 sockets No backup: 2 sockets
Switch time	10 ms
Dimensions (W x D x H)	126 mm x 325 mm x 220 mm
Weight	6 Kg
Control Software	UPSILON 2000
Communication Port	USB
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

INDUSTRIAL/MODULAR UPS

ITEM	REQUIREMENTS
Rating	At least 6 KVA
Input Voltage Swing	Minimum. 220V to 270V
Output voltage	220V - 240V
Output Frequency	50 - 60HZ auto-sensing
Design	automatic voltage regulation
	Mains Isolation
	User replaceable batteries
	Static-Automatic bypass,SMART capabilities enabled
	Maintenance bypass in case of servicing
Battery Module	Minimum 60 minutes backup time on 50% rated output
	Minimum 30 minutes backup time on 100% rated output
	Minimum 5 year lifetime, on Battery
	Type (Sealed lead-acid preferred)
	Automatic periodic battery tests, Front panel mounted fuse
	Short recharge time (Maximum 5 hours for 100% runtime)
	Protection against excessive/damaging discharge
Protection	Output Overload
	Input/Output short-circuit
Form Factor	Rack Mountable
Communication Interface	Asynchronous serial COM port, 10BaseT Ethernet SNMP/HTTP port, Transport Cases, Slides and
Optional accessories	Alternate I/O Configurations, Dual Source Input, Battery Expansion, Battery less Operation, Battery charger/conditioner, power distribution unit, System interface Mounting Kits
Operational environment requirements	Room temperature/humidity (ie. Min. Air Conditioning)
Warranty	At Least 2 years service, replace and Repair
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

APPLICATION SERVER (DEDICATED)

ITEM	REQUIREMENTS
Processor Speed	Intel processor 3.6 GHz duo Core (Two Processors)
Cache Memory	2MB second level ECC cache
Chipset	Intel E7520 Chipset
Memory(RAM)	Minimum:4 GB
Expansion Slots	3 (64-bit/133MHz) PCI-X
Redundancy & Storage Controllers	Support RAID Level 5 (Disk Stripping with Parity) & Smart Array 6i Controller (integrated on system board)
Back Up Functionality	
	Tape Drive & Backup Software
	16X IDE DVD-RW
Internal Storage Capacity	Hot Plug SCSI (3x 146GB)
Display/Graphics	17" TFT Flat Panel LCD, same brand as CPU
Interfaces	1 Serial
	1 Pointing Device (Mouse)
	1 VGA Graphics Adapter
	1 Keyboard
	1 External SCSI
	Dual Port PCI-X 1000T Gigabit Server Adapter (embedded)
	3 USB (1 front, 2 back) & 1 Fire wire interface
Form Factor	Rack Mountable(2U),
Support software, and configuration utilities	Include Server managements manufacturers packs
Power Supply Unit	2 Redundant 500 W Power supply
	Input: 220 - 240 VAC
Warranty	2 Years
SERVER SOFTWARE	
Operating Systems Software	Red Hat Enterprise Linux Advanced server (With open Licenses)
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

STORAGE SERVER (CLUSTERED)

ITEM	REQUIREMENTS
Form factor	12U rack-mount (19")
CPU	Intel® Itanium® 2 Processor; 1.50 GHz/1.60 GHz
Interconnect	Point-to-point crossbar; max data transmission 25.6 gigabits per second
Memory	Max 256GB
Internal Storage	Max 584GB (w/ 2.5" SAS)
PCI Slots	Max 18
Partitions	Max 2
External Dimensions	482 (W) x 820 (D) x 530 (H)
Weight	Max 150 kg
Supported Operating Systems	Red Hat® Enterprise Linux AS (v.4 for Itanium),
	Novell® SUSE® Linux Enterprise Server 9 for Itanium Processor Family,
	Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems,
	Microsoft Windows Server 2003, Datacenter Edition for Itanium-based Systems
Original detailed and highlighted Brochures MUST be submitted	

REPUBLIC OF KENYA

PRESIDENCY AND CABINET AFFAIRS OFFICE
DIRECTORATE OF E-GOVERNMENT
RECOMMENDED MINIMUM TECHNICAL SPECIFICATIONS

TV CARDS

PARTICULARS	GENERAL REQUIREMENTS
Video Input	Able to receive HDTV signals, allowing a system equipped with it to act as a tuner for a connected HDTV-ready device.
Device Type	ATSC HDTV receiver / analog TV / radio tuner / video input adapter
Enclosure Type	Plug-in module
Interface Type	Express Card
VIDEO	
Form Factor	Plug-in module
Interface Type	FM input, S-video input, Composite video input
Analog Video Format	NTSC, PAL-M, PAL-N
Analog Video Signal	S-Video, Composite video
Digital Video Format	MPEG-1, MPEG-2, MPEG-4
Audio Input Support	Standard
Features	Teletext, Sleep timer, Channels preview, Closed captioning, Electronic Program Guide
Audio Input Type	FM tuner - Integrated
Expansion / Connectivity Interfaces	1 x TV antenna - Input, 1 x Display / video - S-video input - 4 pin mini-DIN - External, 1 x Display / video - Composite video input - RCA - External, 1 x Radio - FM input
Software Included	Drivers & Utilities OS Required Microsoft Windows Vista / XP, Peripheral / Interface Devices Sound card, DirectX 9.0c compatible graphics card System Requirements Details - RAM 256 MB - HD 200 MB
Original detailed and highlighted Brochures MUST be submitted	

APPENDIX 2

RECOMMENDED SOFTWARE

2.1 Operating Systems

Category		Type	Recommended software
I.	Desktop OS	Commercial	Windows 7, Windows Vista, Red Hat Enterprise Linux for Desktops or Workstation, Suse Linux desktop
		FOSS	Ubuntu 10.10, Fedora, Free BSD, Linux desktop
II.	Server OS	Commercial	Windows Server 2003, Windows Server 2008, Red Hat Enterprise Server, Suse Linux enterprise, Sun Solaris
		FOSS	Linux, OpenSuse 11.4
III.	Network OS	Commercial/ Proprietary	Junos, Cisco IOS, Extreme XOS, Novel Netware, Windows Server 2003, Windows Server 2008
		FOSS	OpenVMS, Linux, Sun Solaris

2.2 Office Productivity Suites

Category		Type	Recommended software
I.	Office Suite	Commercial	• Ms Office, • Oracle office, • Staroffice for Sun Microsystems.
		FOSS	• open office • Libre Office • Gnome office

2.3 Utilities

Category		Type	Recommended software
I.	Backup	Commercial	• AIMstor Backup • BackupChain • Backup Express (BEX) • Genie Backup Manager
		FOSS	• AMANDA • BackupPC • Bacula
II.	System management software	Commercial	• Tivoli Framework • NetDirector • Cfengine
		FOSS	• Nagios • Fussion • OpenNMS
III.	File management software	Commercial	• SendThru Managed File Transfer • DOC Regenerator

			• Move Me • XYplorer • FindYourFiles
		FOSS	• Filezilla • Restoration • Foxit Reader • Explorer++

2.4 Security software

Category		Type	Recommended software
I.	Endpoint protection systems (Anti-virus, AntiMalware)	Commercial	Norton, Kaspersky Anti-Virus, McAfee VirusScan, Avira AntiVir Personal - Free Antivirus,Panda Antivirus, Panda Antivirus.
II.		FOSS	AVG Anti-Virus, LDAP Directory
III.	Network service management systems	Commercial	CISCO Work VPN/Security Management Solution Cisco IDS software version 3.1
		FOSS	
IV.	Firewall/Intrusion Detection/Intrusion Prevention Systems	Commercial	Checkpoint Integrity, M0n0wall, ZoneAlarm, Windows Firewall KFSensor for Windows
V.		FOSS	Peeruardian, Snort, TripWire, Nessus, SnoopNetCop Standard, Foundstone Attacker, Prevx Home,
VI.	Encryption systems	Commercial	BitArmor for businesses and organizations Guardian Edge for businesses and organizations PGP Whole Disk Encryption for Windows XP and newer Rohos Disk Encryption for Windows XP or newer Steganos Privacy Suite for Windows XP or newer, DriveCrypt, DriveCryptPlus, ShareCrypt
VII.		FOSS	DiskCryptor for Windows XP and newer TrueCrypt for Windows XP and newer, Mac OS X 1.4 and newer, and Linux (kernel 2.4, 2.6, or compatible) Cypherix LE for 32-bit Windows (Vista and earlier) FreeOTFE for Windows XP or newer. AxCrypt,

2.5 Web development and management software

Category		Type	Recommended software
IV.	Content Management Software	**Commercial**	Cold Fusion Microsoft ASP.NET PHP
		FOSS	Joomla, Drupal, Python

V.	Web Development Software	**Commercial**	Adobe Dreamweaver CS Microsoft Visual Studio Photoshop Adobe Image Ready CS
		FOSS	Text Pad Eclipse Aptana Zend Studio
VI.	Web Hosting Software	**Commercial**	Linux Internet Information Service Abyss Web Server Oracle HTTP Server
		FOSS	Apache HTTP Server Nginx Google Web Server Lighttpd Apache Tomcat

2.6 Database software

Category		**Type**	**Recommended software**
	Database	Commercial	Microsoft SQL Server Oracle
		FOSS	MYSQL SQL Express PostgresSQL Apache Derby Openbase

2.7 Communication software

2.7.1 Email Software

Category		**Type**	**Recommended software**
I.	Client Software	Commercial	Microsoft Outlook 2007, Outlook Express, IBM Lotus Notes, Netscape Messenger 9, Novell Evolution
		FOSS	Mozilla Mail and Newsgroups, Mozilla Thunderbird, Incredimail, Eudora, Zimbra Client software, Mdeamon messaging client
II.	Server Software	Commercial	Microsoft Exchange 2007, Netscape Messaging Server, Lotus Domino Mail Server, Novell Groupwise, Sun Java Messaging Server, Lotus Domino, Squid Mail, Exchange.
		FOSS	Zimbra Server software, Fedora Mail, MDeamon messaging server, Squirrel Mail,

2.7.2 Collaboration systems

Category		Type	Recommended software
I.	Server Software	Commercial	IBM Lotus Domino, Oracle Beehive Enterprise collaboration
		FOSS	eGroupware, cynapase, O3spaces, Ourproject.org , Citadel

2.7.3 Voice over Internet Protocol (VoIP).

Category		Type	Recommended software
I.	Client Software	Commercial	CISCO IP communicator, Lotus same time,
		FOSS	Skype, LinPhone, Ekiga , x-lite
II.	Server Software	Commercial	Microsoft Net Meeting, Microsoft Lync 2010, Apple Macintosh iChat, CISCO Unified communications manager, AS5300
		FOSS	GNU Gate Keeper, Free Switch, Astericks

2.7.4 Mobile Messaging Software

Category		Type	Recommended software
I.	Server Software	Commercial	ActiveXpert Software,
		FOSS	Kannel SMS gateway, Rapid SMS

2.7.5 Tele Conferencing /Video Conferencing

CATEGORY		TYPE	RECOMMENDED SOFTWARE
I.	Server Software	Commercial	Adobe Connect, Microsoft NetMeeting, Microsoft Live Meeting, GoToMeeting, InstantPresenter, TandBerg, IBM Lotus Sametime, IBM Lotus live, WebEX
		FOSS	Ekiga, Open H323, AStericks
II.	Client Software	Commercial	Polycom PVX, Sight speed, VSee
		FOSS	Skype, Paltalk, windows live messenger, ooVoo,

2.8 Network Management Software

CATEGORY		TYPE	RECOMMENDED SOFTWARE
I.	Bandwidth Management Software	Commercial	Packet Shaper, Intel's NetStructure 7340 Traffic Shaper , Allot Communication and The Intel NetStructure 7370 Application Shaper
		FOSS	
II.	Network monitoring software	Commercial	• Automated audit trail analysis software • Automated media tracking software • BMC PATROL software • Compaq Insight Manager • Hewlett-Packard HP OpenView software • Integrity verification software • Keystroke monitoring software • Multi-router traffic grapher MRTG software • Network and application load and performance testing software • Network and component performance analysis software • Network availability monitoring software • Network modeling, mapping, and analysis software • Network traffic flow monitoring and analysis software • Network traffic probe software • Network, hardware, and software auditing software • Novell NetWare Management Station • Online traffic calculator software • Packet tracing software • Remote monitoring software • Tcpdump software • ZABBIX software
		FOSS	• AirMagnet Enterprise • Cisco Systems CiscoWorks • Computer-assisted live supervision • Dartware InterMapper • Nagios software • Ethereal • IBM Director • IBM NetView • IBM Tivoli OMEGAMON XE for CICS on z/OS • Ipswitch WhatsUp Gold • Lavalys Everest • Micromuse NetCool • Network monitoring software • Novell NetWare • Performance monitoring tools • Quest BigBrother • Quest Foglight • Sun Microsystems NetManage

GLOSSARY

ADSL	Asymmetrical Digital Subscriber Line - Data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.
Application	Computer programs, procedures, rules, and associated documentation and data pertaining to the operation of a computer system.
ATM	Asynchronous Transfer Mode is a cell-based switching technique that uses asynchronous time division multiplexing.
Audit or Review (Peer Reviews)	An independent review for the purpose of assessing compliance with software requirements, specifications, baselines, standards, procedures, instructions, codes, and other requirements.
Bandwidth	Refers to the speed of a connection between computers. The range of frequencies (size of the 'pipe') available for carrying information. It is the rate of data transfer, throughput or bit rate, measured in bits per second.
Baseline	A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures.
Breadcrumbs	A list of all levels between the home page and the current page, each of which is a link. Listing the levels between the home page and the current page is called the 'breadcrumb' approach which provides context and allows the user to move back up the hierarchy to any level without having to hit all the intermediate points.
Browser	Tool (software programme) that allows users to 'surf the net'.
Campus Infrastructure	Consist of communication systems between groups of buildings within a larger geographical area.
Captcha	This is a type of challenge-response test used in computing as an attempt to ensure that the response is not generated by a computer. The process usually involves one computer (a server) asking a user to complete a simple test which the computer is able to generate and grade.
Cascading Style Sheets	This is a style sheet language used to describe the presentation of the document written in a markup language. Its most common application is to style the web pages written in HTML and XHTML.
Co-location	A dedicated server facility designed with resources which include a secured cage/cabinet, regulated power, dedicated internet connection, security and support.
Computer	A programmable machine that receives input, stores and manipulates data/information, and provides output in a useful format.
Contract Application Programmer	A person or firm who contracts with the GoK to work on an application development product.
CPU	Central Processing Unit - The portion of a computer system that carries out the instructions of a computer program, and is the primary element carrying out the computer's functions.

Data	Groups of information that represents the qualitative or quantitative attributes of a variable or set of variables. Data are often viewed as the lowest level of abstraction from which information and knowledge are derived.
Data Center	A facility housing computer systems and associated components, such as telecommunications and storage systems, centrally. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g. air conditioning, fire suppression) and security devices.
Download	Transfer of data from a server to a user's computer hard disk.
E-commerce	The process of conducting a financial transaction through electronic means, e.g. using an EFTPOS card, purchasing goods over the Internet. (EFTPOS – Electronic Fund Transfer Point of Sale)
E-form	Electronic Form is a computer program version of a paper form. E-forms are filled out faster because the programming associated with them can automatically format, calculate, look up, and validate information for the user.
Email	Messages, usually text, sent from one person to another via electronic medium. Email may also be sent automatically to a large number of addresses (mailing list).
Encryption	The process of transforming information (plain text) using an algorithm to make it unreadable to anyone except those possessing special knowledge.
Evaluation	A technique in which requirements, design, code and test results are examined in detail by a person or group to detect problems. The results are documented.
Extranet	An intranet or portion of an intranet to which an MDA allows access by selected external entities, who could be partners of the MDA.
E-waste	Electronic waste.
FAQs	Frequently Asked Questions.
FOSS	Free and Open Source Software
Firewall	Internet security to protect a LAN (Local Area Network) against hackers. A combination of hardware and software acts as a firewall to separate the LAN into two parts. "Normal" data is available outside the firewall, while more private or confidential material is inside.
Forms	In this context, electronic forms that can be filled in for different purposes (e.g. for downloading, providing feedback, registering for a service).
Gateway	Hardware or software that translates between two dissimilar protocols.
Hardware	The physical artifacts of a technology i.e. the physical components of a computer system, in the form of computer hardware.
Hits	A count of all successful hits including HTML pages, pictures, forms, scripts, and downloaded files. It is not recommended as a means of counting website usage. `Visitor sessions' provide a more accurate picture of the number of users for a website.
Home Page	The primary or main web page for an MDA.
Host	The server on which a website is stored.
HTML	Hyper Text Markup Language: The coding language to create hypertext documents on the web.
HTTP	Hyper Text Transport Protocol: The protocol for moving hypertext files across the Internet.

Hypertext	This is text that contains 'links' to other documents.
IDS	Intrusion Detection System - Combination of hardware and software products that are used to analyze network traffic passing through a single point on the network.
Indexing agents	Indexing agents such as 'spiders' and web 'robots' are computer programs that roam the Internet scanning and summarizing web pages and storing this information into their associated databases. Search engines use this information to locate web pages which help consumers to easily find websites depending on how effectively these agents index and summarize the websites.
Internet	A network of computer networks that communicates utilizing TCP/IP protocols.
Intranet	A 'closed Internet' for internal use only, also utilizing TCP/IP protocols and browser software.
IP	Internet Protocol: The rules that provide basic Internet functions. IP allows computers to find each other. It is the set of communications protocols used for the Internet and other similar networks.
IP address	A 32bit Internet address consisting of four numbers separated by dots and sometimes called a "dotted quad". Every server connected to the Internet has an IP address.
IPAD	
IPS	Intrusion Prevention system - A network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.
IP/MPLS	Refers to a network backbone that uses the IP protocol augmented with MPLS.
LAN	Local Area Network – Computer network covering a small physical area, like a home, office, or small groups of buildings, such as a school, or an airport.
Log	A file that keeps records of a website's or a server's activity. The file that contains information on how many visitors a web page is getting.
Maintenance	To repair, change, or add to a software product.
MAN	Metropolitan Area Network – A large computer network that usually spans a city or a large campus.
Megabyte (MB)	A measure of amount of information used.
Metadata	Data about data information describing the content of a resource and its intellectual property rights.
Mirror	More or less an exact copy of another Internet or FTP website. Mirror websites are created when the traffic on the original website is too heavy. They are usually on servers that are located in different geographic areas.
Network	A collection of terminals, computers, servers, and components which allows for the easy flow of data and use of resources between one another.
Network Architecture	The design of a communications system, which includes the backbones, routers, switches, wireless access points, access methods and protocols used.
Online	In this context, actions performed when connected to the Internet.
Online services	Services accessed through the use of electronic technology, with an emphasis on Internet and telecommunications technology.

OSI	Open System Interconnection - A way of sub-dividing a System into smaller parts (called layers) from the point of view of communications.
Page visits	Total count of hits to web pages.
PDF	Portable Document Format: A file format that captures all the elements of a printed document as an electronic image that can be viewed, navigated, printed, or forwarded to someone else.
Plug-in	A hardware or software module that adds a specific feature to a larger system. The added feature simply plugs in to the existing system.
Portal	A comprehensive and standardized system integrating all government online services, presenting information from different sources in a unified way.
Privacy	The rights and obligations of individuals and organizations with respect to the collection, use, disclosure and retention of personal information.
Product	A product is the tangible result of any process or work group. This includes, but is not limited to, shrink-wrapped or other software products, components, code, services, and deliverables.
Project	A collaborative enterprise, frequently involving research or design that is carefully planned to achieve a particular aim.
Protocol	An agreement relating to systems which allow computers to communicate together. It is a set of rules which is used by computers to communicate with each other across a network
PTAD	Project Team for Application Development. A group of people representing different disciplines who collaborate and work together to deliver an application development product.
RAD	Rapid Application Development - A type of software development methodology that uses minimal planning in favor of rapid prototyping.
SDLC	Software Development Lifecycle - A structure imposed on the development of a software product. The SDLC is a systematic approach to the creation of software or application. This cycle typically includes a requirements, analysis, design, coding, test, implementation and post-implementation phases.
Security	Protection of data from accidental or intentional but unauthorized modification, destruction or disclosure through the use of physical security, administrative controls, logical controls and other safe guards to limit accessibility.
Search Engine	A web search facility designed to search for information on the World Wide Web.
Server	In this context, a host computer providing the website information.
Sign-off	The term used to describe a point in the application development process where an individual/governance agency officially approves and accepts the product.
Site Map	A list of pages of a web site accessible to crawlers or users.
SNMP	Simple Network Management Protocol – Used in network management systems to monitor network-attached devices for conditions that warrant administrative attention
Software	The collection of computer programs and related data that provide the instructions telling a computer what to do.
Splash Pages	These are graphically rich entry pages used to attract attention and develop brand recognition. They often consist of sophisticated animated displays and

	prompt users to "click here to enter the website". This can often lead to frustration through delay.
SQL	Structured Query Language - A database computer language designed for managing data in relational database management systems, and originally based upon relational algebra.
SPSS	Statistical Package for the Social Sciences.
Standard	An established norm or requirement.
Strategy	A plan of action designed to achieve a particular goal.
T1/T3	Leased lines used in long-distance computer networking.
TCP/IP	Transmission Control Protocol/Internet Protocol: A suite of communications protocols that defines the basic workings of the Internet i.e. how computers on the Internet exchange information.
URL	Uniform Resource Locator: This is an address of any resource on the World Wide Web.
VPN	Virtual Private Network: A private data network that makes us the public network/infrastructure i.e. Internet. Privacy is maintained by employing secure protocols and security procedures, such as data encryption. A VPN encapsulates data transfers between two or more networked devices not on the same private network so as to keep the transferred data private from other devices on one or more intervening local or wide area networks.
Walk-through	A review process in which an individual(s) lead their peers through their work product.
WAN	Wide Area Network – A Computer network that covers a broad area, any network whose communications links cross metropolitan, regional, or national boundaries.
Web page	A document with a single URL.
Webmaster	The technical person responsible for the managing and running of the web environment for the MDA.
Website	A website is one or more web pages with a related set of URLs that are controlled by a single administrative entity.