KISII COUNTY GOVERNMENT

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) STANDARDS

JUNE 2020

1 Table of Contents

Foreword 6
1 Introduction 7
2 Domains 8
3 End-User Computing Devices 9
3.1 Introduction 9
3.2 End-User Requisition 9
3.3 Technical Specifications 9
3.4 Technical Evaluation 10
3.5 Bring Your Own Device (BYOD) 10
3.6 Inventory 11
3.7 Maintenance 11
3.8 Decommissioning 12
3.9 Data Protection 12
3.10 Minimum Hardware Specifications 12
3.10.1 Desktop Computer 12
3.10.2 Laptop Computer 13
3.10.3 MacBook Computer 13
3.10.4 Notebook Computer 14
3.10.5 Tablet Computer 15
3.10.6 Laser Printer 16
3.10.7 Colour Laser Printer 17
3.10.8 Scanner 17
3.10.9 Small Office Photocopier 18
3.10.10 Medium Office Photocopier 19
3.10.11 Large Office Photocopier 20
3.10.12 Multi-Purpose Photocopier 21
3.10.13 Wall-Mounted LCD Projector 23
3.10.14 Portable LCD Projector 24
3.10.15 LCD Display Panel 24
3.10.16 DSLR Digital Camera 25
3.10.17 Compact Digital Camera 26
3.10.18 Digital Camcorder 27

3.10.19 Digital Video Camera 28
3.10.20 Standby UPS 29
3.10.21 Smart/Online UPS 30
3.10.22 Industrial/Modular UPS 31
3.11 Accessibility by Persons with Disability 31
3.11.1 Usage without vision 31
3.11.2 Usage with limited vision 31
3.11.3 Usage without perception of colour 32
3.11.4 Usage without hearing 32
3.11.5 Usage with limited hearing 32
3.11.6 Usage without vocal capability 32
3.11.7 Usage with limited manipulation or strength 32
3.11.8 Usage with limited reach 33
3.11.9 Usage with photosensitive seizures 33
3.11.10 Usage with limited cognition 33
3.11.11 Privacy 33
4 Software Acquisition, Maintenance and Disposal 34
4.1 Introduction 34
4.2 Project Management 34
4.2.1 Project Plan 34
4.2.2 Project Scope 34
4.2.3 Project Status Reporting 34
4.2.4 Roles and Responsibilities 34
4.2.5 Analysis and Design 34
4.3 Acquisition 35
4.3.1 Procurement 35
4.3.2 In-house Development 35
4.3.3 Outsourced Development 36
4.3.4 Commercial Off-The-Shelf Software 36
4.4 Development 36
4.4.1 Skills 37
4.4.2 Documentation 37
4.4.3 Security 37

4.4.4 Testing 37
4.5 Maintenance 37
4.5.1 Change Management 38
4.5.2 Licences 38
4.5.3 Updates 38
4.5.4 Support 38
4.5.5 Security Audit 38
4.5.6 Training and Knowledge Transfer 38
4.6 Disposal 39
5 Messaging and Collaboration 41
5.1 Introduction 41
5.2 General Requirements 41
5.3 Email 41
5.4 Audio and Video Conferencing 42
5.5 Social Media 42
6 Networks 43
6.1 Introduction 43
6.2 Definitions 43
6.3 Telecommunication Rooms, Pathways and Spaces 44
6.4 Network Design, Configuration, Documentation and Commissioning 44
6.5 Network Monitoring and Management 44
6.6 Preventive Maintenance 45
6.7 Wireless Network Connectivity 45
6.8 Internet 45
6.9 Network Security 46
7 Cloud Computing 47
7.1 Introduction 47
7.2 Definitions 47
7.3 General Requirements 48
7.4 Auditability 50
7.5 Interoperability 50
7.6 Maintenance and Versioning 51
7.7 Performance 51

7.8 Portability 51
7.9 Protection of Personally Identifiable Information 52
7.10 Resilience 52
7.11 Reversibility 52
7.12 Security 52
7.13 Service Level Agreements 53
8 Information Security 54
8.1 Introduction 54
8.2 Cybersecurity Management 54
8.2.1 Mobile Device Management 54
8.2.2 Teleworking 55
8.2.3 Malware Defence 55
8.2.4 Administrative Privileges 56
8.3 Systems and Applications Security 56
8.3.1 Systems Acquisition and Development 56
8.4 Communication Security 57
8.4.1 Network Security 57
8.4.2 Wireless Security 59
8.4.3 Electronic Messaging 59
8.4.4 Information Sharing 60
8.4.5 Information Transfer 60
8.5 Risk Management 61
8.5.1 Information Asset Management 61
8.5.2 Information Classification and Sharing 63
8.5.3 Information Backup 64
8.5.4 Business Continuity and Disaster Recovery Plan 65
8.5.5 Threat and Vulnerability Management 66
8.6 Human Resource Security 67
8.6.1 Background Screening 67
8.6.2 In-Service 67
8.6.3 Termination or Change of Responsibilities 67
8.6.4 Information Security Awareness 68
8.7 Operational Control 68

8.7.1 User Access Management 68
8.8 Physical and Environment Security 71
8.9 Cloud Security 72
Abbreviations 73

Foreword

<< to be drafted by the CEC in charge of ICT>>

1 Introduction

ICT standards provide comprehensive and rigorous approaches to managing the complexities of ICT systems. The application of ICT has enabled the transformation and automation of operations and services, enabling improvements in performance and quality of service. However, the quick and constant evolution of products can negatively impact the stability of business processes. Standards support the unification of practices and set acceptable limits on technologies employed by an organization to mitigate such risks.

ICT standards can be characterized in the following ways:

i. ***Solutions standards*** specify the types of ICT products that can be used (according to manufacturer, version, platform or other defining characteristics), as well as the process by which these standardized products are acquired.

ii. ***Configuration standards*** specify the way selected devices, software and applications are installed and configured.

iii. **Utilization standards** specify the applicability of a given ICT product (or set of products) to a demonstrated, stated operational need, forming the basis of ICT planning, procurement and product selection recommendations.

The standards outlined in this document are aimed at supporting the Kisii County Government in the application of systematic and consistent ICT practices, and providing a general framework for the application of the standards across the County.

By planning and applying the right set of standards, the Kisii County Government can realize several benefits across a broad spectrum. These include, but are not limited to:

i. With a focus on a specific set of ICT products, end users will have the opportunity to develop in-depth product expertise to enhance operational productivity and maximize technology utilization.

ii. By limiting the variety of ICT products in use, ICT departments can better test and manage product compatibility, thereby reducing the number of platform conflict problems.

iii. Standardization can lower ICT acquisition costs through volume purchasing, bringing discounted pricing, as well as greater leverage to negotiate more favourable maintenance and training contracts.

iv. Standardization can minimize risks associated with uncontrolled technology portfolio, facilitating disaster recovery planning, software licensing management and security management.

2 Domains

The following are the domains covered by these standards:

1. End-User Computing Devices
2. Software Acquisition, Maintenance and Disposal
3. Messaging and Collaboration
4. Networks
5. Cloud Computing
6. Information Security

3 End-User Computing Devices

3.1 Introduction

The KCG uses end-user computing devices such as personal computers (e.g. desktops and laptops), peripheral devices (e.g. printers, photocopiers and projectors) and removable storage media (e.g. flash disks, external hard disks, memory cards) to support administrative functions.

This standard establishes guidelines for security, acquisition, support, and disposal of all end-user devices and services by the KCG. It provides technical guidance for procuring and implementing end-user computing devices with the following goals in mind:

i. Ensure the KCG receives value for money.
ii. Ensure compatibility and interoperability.
iii. Easy maintenance.
iv. Cost-effective use of computing resources by sharing wherever possible.
v. Consistency in equipment functionality.
vi. Improved end-user experience.

3.2 End-User Requisition

a. The ICT department 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.
b. The ICT department shall ensure that requests for procurement and acceptance of ICT equipment is validated by the head of the department.
c. Personal communication devices (PCDs) shall be issued only to personnel with duties that require them while away from their normal work locations.
d. Requisition of handheld wireless devices shall be restricted to personnel whose duties justify their use for operational efficiency.

3.3 Technical Specifications

a. The KCG shall ensure that acquired equipment has a useful life of not less than five years (total lifecycle).
b. The KCG shall specify equipment functionality to guarantee that operational requirements intended to be performed by ICT equipment can be achieved effectively with the equipment specified.
c. The KCG shall provide security specifications to address the need to protect equipment, system data and the operational environment from loss or compromise.
d. The KCG shall provide interoperability requirements to facilitate the exchange of information between potentially heterogeneous systems through conformance to open standards.
e. The KCG shall provide compatibility requirements of ICT equipment components to effectively and efficiently work together in an integrated system.

f. The KCG shall provide scalability requirements to ensure that acceptable ICT components enhance the ability of the equipment to support future growth and increased throughput.
g. The KCG shall provide availability requirements to maintain acceptable operational levels.
h. The KCG shall provide accessibility requirements that will facilitate the users and operators to access the equipment in a timely fashion and perform its intended functions.
i. Where the service is outsourced, support arrangements shall be made to ensure availability of vendor and/or internal support, including parts and labour (where applicable).
j. The KCG shall provide upgradability requirements to ensure ICT component installations that need updates are updated to the latest official versions available.
k. The KCG shall purchase equipment with the latest stable technology to guarantee that the devices are based on the latest technology in the market (where applicable).

3.4 Technical Evaluation

a. ICT equipment that does not meet industry and safety standards shall be prohibited from being deployed. All donations should meet the minimum specifications.
b. Technical evaluation shall be undertaken to ensure that the equipment is fit for the intended purpose and that it meets the required specifications.
c. The head of the KCG ICT department shall participate as a technical lead in the technical evaluation and inspection processes for all end-user computing devices.
d. All ICT equipment and assets (whether new, transferred and/or written off), shall be recorded by the ICT department for audit and other asset managerial purposes.
e. The head of the ICT department shall ensure that agreements on warranty, technical support and guarantees are provided and shall also oversee their administration. The minimum warranty for all ICT equipment shall be three years.
f. Before installation, the equipment must be tested to ensure they work as per the specifications and associated licensing for the equipment validated.
g. The equipment shall be deployed and used for the intended purpose. Only qualified personnel shall be allowed to install ICT equipment.
h. The installation of ICT equipment shall adhere to the OEM instructions. Only trained and qualified personnel will be allowed to operate the ICT equipment.
i. ICT equipment shall be operated within the environmental conditions (temperature, humidity, etc.) recommended by the OEM.
j. Access and maintenance of equipment shall only be carried out by authorized and accredited personnel.
k. All new end-user devices (e.g. PCs and Notebooks) shall be supplied with the software installations (where applicable).

3.5 Bring Your Own Device (BYOD)

a. The deployment and use of personal devices shall be approved by the ICT department.

b. The KCG shall ensure that users of personal devices are authenticated, data/information protected/encrypted to limit transfer of county government data to unauthorized entities; and such personal devices shall have updated antivirus and licensed software.

3.6 Inventory

a. All equipment and assets whether new, donated, transferred and/or written off shall be recorded and tagged appropriately by the ICT department for audit and other asset managerial purposes.
b. The inventory of ICT assets shall indicate product details (product number, serial number, part number, etc.), tracking information, maintenance schedules and warranty information.
c. Officers exiting the KCG shall be required to surrender all ICT equipment in their custody to the County Government.
d. The KCG shall endeavour to automate the end-user equipment inventory.

3.7 Maintenance

a. ICT equipment maintenance may be done in-house by the ICT department where a maintenance function is established.
b. Sub-contracting for maintenance shall be through appropriate justification and approval by the accounting officer in consultation with the ICT department. Due diligence shall be undertaken in engaging and retaining such contractors. Contractors shall also sign an NDA.
c. ICT department shall develop schedules for maintenance, replacement and upgrading plans for end-user devices. The schedules shall specify the frequency and types of maintenance for each type of equipment. In case of mission-critical equipment, users shall be notified of the maintenance in advance.
d. The KCG shall develop, negotiate and enforce SLAs to guarantee maintenance of end-user devices. Vendor's SLAs terms shall ensure value for money to the KCG.
e. The KCG shall ensure that end-user devices are provided with clean power to protect against damage in the event of power fluctuations.
f. The ICT department shall undertake regular surveys to identify obsolete equipment for the purposes of disposal. Where such equipment contains data, that data shall be backed up and then erased from the device using suitable mechanisms (e.g. equipment sanitization) in line with information standards.
g. The ICT department shall electronically track the physical locations and status of all equipment where possible.
h. ICT equipment maintenance shall consider routine preventive or corrective upgrades, and repair maintenance as may be required.
i. The ICT department shall periodically conduct assessment/audit of ICT equipment to ensure compliance with performance standards and requirements, and ensure equipment component parts are as indicated in the inventory.

3.8 Decommissioning

a. The ICT department may decommission equipment that is no longer needed in its ICT environment. Decommissioning of equipment shall be undertaken through committee. The decommissioning should be in line with the Procurement and Assets Disposal Act.
b. Equipment may be decommissioned if: it becomes redundant; it becomes technologically obsolete; it has insufficient capacity to handle application and/or user requirements; where upgradability options have been exhausted; where equipment has become unsafe. The equipment can also be reassigned to lesser demanding tasks or appropriate environment if it meets the required safety standards
c. The ICT department may dispose of equipment that it deems no longer useful, damaged beyond repair, cannot be upgraded, the repair cost is higher than the cost of buying a new one, the parts and/or consumables are not available and end of life and no longer supported by the OEM.
d. The ICT department may recommend disposal via donation, trashing, selling, and cannibalizing, in which case proper records shall be kept to indicate where such components are used or stored.

3.9 Data Protection

End user equipment data protection shall be in line with information security standards.

3.10 Minimum Hardware Specifications

3.10.1 Desktop Computer

Feature	Specifications
Processor	Intel Core i5 (2.20-GHz, 3 MB L2 cache, 1066- MHz FSB) or Higher LGA 1156
Memory	At least 4GB
Storage	At least 500GB
Form Factor	Micro Tower All-in-One
Display/Graphics	17" TFT Flat panel Colour LCD, Same brand as CPU
	1024x768(16:9), with EnergyStar rating
Optical Drives	16X Dual Layer DVD+/-RW
Keyboard and Pointing Device	1 x USB Enhanced keyboard
	1 x USB Optical Wheel Mouse
Audio	Stereo audio system with 2 speakers
	2 x Audio ports: headphone and microphone
Communication interface	100/1000 Mbps Gigabit Ethernet
	56K ITU V.90 data/fax modem, wake-on-ring ready
I/O interface ports	6x High speed USB 2.0 (2 front/4 rear)
	1x 25 Pin Parallel Port
	1x RJ45 jack for Ethernet
	1x External VGA-in Port
Operating System	Windows 10 pre-installed (with licensed CD or backup CD)
Software	Office 2019 (with licensed CD)

	Latest antivirus software (with licensed CDs)
Power supply	220 – 240v AC, 50/60 Hz(auto-sensing)
Warranty	One (1) Year
Original detailed and highlighted brochures must be submitted	

3.10.2Laptop Computer

Feature	Specifications
Processor	Intel Core i5 (2.20GHz, 3MB L3 Cache FSB) or higher
Memory	At least 4GB
Storage	At least 500GB
Optical Drives	16X 9.5mm DVD+/-RW multi burner
Keyboard and Pointing Device	Enhanced keyboard
	USB Optical Wheel Mouse
Audio	Stereo audio system
	Combo microphone in/audio out
Communication interface	10/100/1000Mbps Gigabit Ethernet
	802.11 a/g/n (WPA2 Enterprise-compatible)
I/O interface ports	At least 3 USB 2.0 ports
	1x RJ45 jack for Ethernet
	1x External VGA Port / HDMI port
Operating System	Windows 10 (with licensed CD or backup CD)
Software	Office 2019 (licensed with CD)
	Latest antivirus software (with licensed CDs)
Accessories	Executive leather carry case
Power Subsystem	Power management standard to support standby and Hibernation
	Power saving modes
	6-cell 60Wh battery pack, 4 hours battery life
	1 AC Power Connector
Warranty	One (1) Year
Original detailed and highlighted brochures must be submitted	

3.10.3MacBook Computer

Feature	Specifications
Processor	Intel Core i5 or i7 or AMD 2.20GHz, with 6MB shared L3 cache;
	1066MHz –data Bus
Memory	At least 4GB
	DDR3 SDRAM –1066MHz
Storage	At least 500GB
Power System	Power management standard to support standby and Hibernation
	Power saving modes

	6-cell 60Wh battery pack, 4 hours battery life (when unplugged)
	1 AC Power Connector
Display/Graphics	15.4” TFT Colour LCD, LCD display at 1440x900
	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	10/100/1000 Mbps Gigabit Ethernet, RJ45 jack,
	802.11 a/g/n (WPA2 Enterprise-compatible)
I/O interface ports	1x Audio - SPDIF Input
	1x Audio - SPDIF Output
	1x 9 Pin Serial Port
	1x 25 Pin Parallel Port
	4x USB Port
	1x External VGA Port
Operating System	macOS 10.15
Accessories	Carry Case, Mouse
Warranty	One (1) Year
Original detailed and highlighted brochures must be submitted	

3.10.4Notebook Computer

Feature	Specifications
Processor	At least 2.0 GHz Intel Core i5M L2 Cache or equivalent
Memory	At least 4GB
Storage	At least 320GB
Power System	Power management standard to support standby and Hibernation power saving modes
	60Wh battery Pack,
	At least 4-hour Battery life (when unplugged)
	1 AC Power Connector
Display Graphics	14" TFT Colour LCD, 1024x768
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	4x USB 2.0 ports

	1x External VGA or HDMI Port
	1x AC Power Connector
Operating System	Windows 10 (with licensed CD or backup CD)
Software	Office 2019 (with licensed CD)
	Latest antivirus software (with licensed CDs)
Accessories	Carry Case, power adapters, external optical mouse
Warranty	1 Year Onsite Repair & Replace
Original detailed and highlighted brochures must be submitted	

3.10.5Tablet Computer

Feature	Specifications
Notebook Tablet series	Handwriting and voice recognition enabled. Handwriting must be digitized with an industry standard WACOM digitizer.
Processor and core Logic	Intel® CoreTM2 Duo Processor L7500 (2.2GHz, 4MB, 800MHz)
Weight	1.20 kg (2.1 lb) or (2.6 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-ion Battery life
Display Graphics	12.1" TFT super-wide Angle with Anti- Reflective/Anti-Glare Protective Coatings Colour LCD, 1024x768
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)
	RJ11 Port (Modem)
	Bluetooth and wireless technology
I/O Interface	3x USB ports
	1x External VGA Port
	1 AC power
	Battery life of up to 6.3 hours on 8-cell Li-ion Battery life
Operating System	Windows 10 (with licensed CD or backup CD)
Software	Office 2019 (with licensed CD)
	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	

3.10.6Laser Printer

Feature	Specifications
Print Quality	1200x1200 dpi
Print Speed and throughput	Up to 45 ppm black
Print technology	Laser black
Memory	1GB or higher, expandable
Memory slots	2x 100-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 trays
	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, A4 and 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
Compatible Operating Systems	Windows 7/8/10; Windows Server 2012/2016/2020; macOS; Linux
Software included	Print drivers and installation software on CD- ROM, PCL6, PostScript Level 3 emulation
Warranty	One year
Original detailed and highlighted brochures must be submitted	

3.10.7Colour Laser Printer

Feature	Specification
Print speed, black (best quality mode)	40ppm
Print speed, black (normal quality mode)	40 ppm
First page out (black)	As fast as 10 sec
First page out (colour)	As fast as 10 sec
Monthly duty cycle	Up to 100,000 pages
Print resolution, black	Up to 600 x 600 dpi
Print resolution, colour	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	Windows 7/8/10; Windows Server 2012/2016/2020; macOS; 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	

3.10.8Scanner

Feature	Specifications
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/colour)
Scanning Technology	Dual CCD
	Grayscale output bit depth is 256 levels (8- bit)
	Colour capture bit depth is 48 bits (16x3)
	Colour output bit depth is 24 bits (8x3)
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	34–413 g/m2 (9–110 lb.) paper

Weight	
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 colour dropout; dual stream scanning; interactive colour, brightness and contrast adjustment; automatic orientation, automatic colour detection, background colour 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, 3GB RAM
Supported Operating Systems	Windows 7/8/10; Windows Server 2012/2016/2020; macOS; Linux
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	

3.10.9Small Office Photocopier

Feature	Specifications
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
Memory	Minimum 256 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	50/60 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	Multi-position 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	

3.10.10 Medium Office Photocopier

Feature	Specifications
Copying / Print technology	Laser
Duplex copying/printing	Two-sided copying Automatic
Input: Output support	1-1, 1-2, 2-1, 2-2.
Copying Speed	30cpm
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
Bypass 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	

3.10.11 Large Office Photocopier

Feature	Specifications
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)	2GB
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 (11x17 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	50/60 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	

3.10.12 Multi-Purpose Photocopier

Feature	Specifications
All-in-one functions	Print, copy, Scan and Fax
Multitasking capability	Yes
Printer Specifications	
Print technology	LaserJet
Print speed, black (normal quality mode)	Up to 40 ppm
Print speed, colour (normal quality mode)	Up to 40 ppm
First page out (black)	As fast as 11.5 sec
First page out (colour)	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, colour	Up to 1200 x 600 dpi
Memory	512 MB
Processor speed	835 MHz
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 an 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, colour	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
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	Windows 7/8/10; Windows Server 2012/2016/2020; macOS; Linux
Warranty	1 year
Original detailed and highlighted brochures must be submitted	

3.10.13 Wall-Mounted LCD Projector

Feature	Specifications
Resolution	XVGA 1024x768 pixels
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	1x RGB, 1x Audio, PC control, Screen control, 1x S-video
Audio	2x 2.5W 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, 1500 hours
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	100 cm x 700 cm diagonal
Original detailed and highlighted brochures must be submitted	

3.10.14 Portable LCD Projector

Feature	Specification
Display Technology	3LCD
Max number of colours	16.7 Million
Projector Brightness	At least 2500 ANSI Lumens
Resolution	At least 1024x768 Pixels
Supported Resolution	Up to 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 x 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	

3.10.15 LCD Display Panel

Feature	Specifications
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)
	HDMITM 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 - 8MS
	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
Power Consumption (in Operation)	Approx. 320W
Power Requirements	AC 100-240V, 50/60Hz
HDMITM Technology	No (Available through Option Card BKM-FW15)
Multiple Language Display	English, French, Spanish, Italian, German, Japanese, Dutch, Swedish, Russian, Chinese
On-Screen Display	Picture and Picture
	Yes
	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	Colour Temperature Control
	Colours
	Operating Humidity
	Operating Temperature
	Screen Treatment
PC Connection	Computer display with support for resolutions up to 1920 x 1080 through HDMI and VGA

3.10.16 DSLR Digital Camera

Feature	Specifications
Resolution	14.1 Megapixels
sensor type	CMOS
Image Stabilization	Standard
Image Resolution	4320 x 3240
Minimum Shutter	60 sec

speed	
Minimum continuous shooting speed	3.5 frames per second
Video capture	1280x720; 640x480; 320x240
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
Operating Systems compatibility	Windows 7/8/10; Windows Server 2012/2016/2020; macOS; Linux
Warranty	1 year
Original detailed and highlighted brochures must be submitted	

3.10.17 Compact Digital Camera

Feature	Specifications
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	1280x720; 640x480; 320x240
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	Windows 7/8/10; Windows Server 2012/2016/2020; macOS; Linux
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	

3.10.18 Digital Camcorder

Feature	Specifications
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	

3.10.19 Digital Video Camera

Feature	Specifications
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	12x
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 1920x1440, JPEG 1440x1080, JPEG 1920x1080, JPEG 640x480
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	1x Component video output, 1x Composite video/audio output, 1x S-Video output, 1x Headphones, 1x Audio input, 1x Control-L (LANC), 1x USB, 1x 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 colour 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	

3.10.20 Standby UPS

Feature	Specifications
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 regulation
	Mains Isolation
	User replaceable batteries
	Static-Automatic bypass
	Run time (full load) 2,4 min
	Maintenance bypass in case of servicing
Battery Module	Minimum 16 minutes backup time on 50% rated output
	Minimum 5 minutes backup time on 100% rated output
	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	

3.10.21 Smart/Online UPS

Feature	Specifications
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 Phase)	230Vac + 10% - 15%50Hz 5% in-line
Power (kVA/KW)	850Va/500W
Output number	Back: 2 IEC sockets + 2 sockets No backup: 2 sockets
Switch time	10ms
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	

3.10.22 Industrial/Modular UPS

Feature	Specifications
Rating	At least 6 KVA
Input Voltage Swing	Minimum. 220V to 270V
Output voltage	220V - 240V
Output Frequency	50 - 60HZ auto-sensing
	Automatic voltage regulation
	Mains Isolation
Design	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 (i.e. Min. Air Conditioning)
Warranty	At Least 2 years service, replace and repair
Original detailed and highlighted brochures must be submitted	

3.11 Accessibility by Persons with Disability

3.11.1 Usage without vision

Where ICT equipment provides visual modes of operation, some users need the equipment to provide at least one mode of operation that does not require vision.

NOTE 1: Audio and tactile user interfaces may contribute towards meeting this clause.

3.11.2 Usage with limited vision

Where ICT systems provide visual modes of operation, some users will need the system to provide features that enable users to make better use of their limited vision.

NOTE 1: Magnification, reduction of required field of vision and control of contrast, brightness and intensity can contribute towards meeting this clause.

NOTE 2: Where significant features of the user interface are dependent on depth perception, the provision of additional methods of distinguishing between the features may contribute towards meeting this clause.

NOTE 3: Users with limited vision may also benefit from non-visual access (see clause 3.11.1).

3.11.3 Usage without perception of colour

Where ICT systems provide visual modes of operation, some users will need the system to provide a visual mode of operation that does not require user perception of colour.

NOTE 1: Where significant features of the user interface are color-coded, the provision of additional methods of distinguishing between the features may contribute towards meeting this clause.

3.11.4 Usage without hearing

Where ICT systems provide auditory modes of operation, some users need the system to provide at least one mode of operation that does not require hearing.

NOTE 1: Visual and tactile user interfaces may contribute towards meeting this clause.

3.11.5 Usage with limited hearing

Where ICT systems provide auditory modes of operation, some users will need the system to provide enhanced audio features.

NOTE 1: Enhancement of the audio clarity, reduction of background noise, increased range of volume and greater volume in the higher frequency range can contribute towards meeting this clause.

NOTE 2: Users with limited hearing may also benefit from non-hearing access (see clause 3.11.4).

3.11.6 Usage without vocal capability

Where ICT systems require vocal input from users, some users will need the system to provide at least one mode of operation that does not require them to generate vocal output.

NOTE 1: This clause covers the alternatives to the use of orally-generated sounds, including speech, whistles, clicks, etc.

NOTE 2: Keyboard, pen or touch user interfaces may contribute towards meeting this clause.

3.11.7 Usage with limited manipulation or strength

Where ICT systems require manual actions, some users will need the system to provide features that enable users to make use of the system through alternative actions not requiring manipulation or hand strength.

NOTE 1: Examples of operations that users may not be able to perform include those that require fine motor control, path dependent gestures, pinching, twisting of the wrist, tight grasping, or simultaneous manual actions.

NOTE 2: One-handed operation, sequential key entry and speech user interfaces may contribute towards meeting this clause.

NOTE 3: Some users have limited hand strength and may not be able to achieve the level of strength to perform an operation. Alternative user interface solutions that do not require hand strength may contribute towards meeting this clause.

3.11.8 Usage with limited reach

Where ICT products are free-standing or installed, the operational elements will need to be within reach of all users.

NOTE 1: Considering the needs of wheelchair users and the range of user stature in the placing of operational elements of the user interface may contribute towards meeting this clause.

3.11.9 Usage with photosensitive seizures

Where ICT systems provide visual modes of operation, some users need the system to provide at least one mode of operation that minimizes the potential for triggering photosensitive seizures.

NOTE 1: Limiting the area and number of flashes per second may contribute towards meeting this clause.

3.11.10 Usage with limited cognition

Users with limited cognitive, language and learning abilities will need the ICT system to provide features that make it simpler and easier to use.

NOTE 1: Adjustable timings, error indication and suggestion, and a logical focus order are examples of design features that may contribute towards meeting this clause.

3.11.11 Privacy

Where ICT systems provide accessibility features, some users will need their privacy to be maintained when using those systems.

NOTE 1: Enabling the connection of personal headsets for private listening, not providing a spoken version of characters being masked and enabling user control of legal, financial and personal data are examples of design features that may contribute towards meeting this clause.

4 Software Acquisition, Maintenance and Disposal

4.1 Introduction

This section covers standards for developing/purchasing, installing and maintaining software applications in the KCG. These standards apply to any department or vendor engaged by the KCG that undertakes development, installation or maintenance of ICT applications. The determination for when these standards apply depends on the nature of the application, not on who is responsible for the development.

4.2 Project Management

Project management refers to the organization of resources to achieve specific outcomes within given cost and schedule constraints. Project management spans across all phases of systems development. It generally consists of planning, initiation, execution, monitoring and closing of a project.

4.2.1 Project Plan

The KCG shall ensure that each project has a plan to guide its implementation and reduce the likelihood of major, unexpected cost or schedule overruns. The plan must be updated regularly throughout the development process to reflect any changes or refinements encountered.

4.2.2 Project Scope

The KCG shall establish the overall scope of the project early in the development cycle with a project leader appointed to be the custodian of the approved scope. If major issues arise regarding the scope of the project, then senior level management may need to become involved to determine whether the scope should be expanded significantly.

4.2.3 Project Status Reporting

As part of the management of projects, the project leader must provide regular status reports to the accounting officer for each significant development project. The report should address progress on meeting major milestones, changes in estimated completion dates for future milestones, any issues encountered and review of the remaining tasks.

4.2.4 Roles and Responsibilities

The KCG shall identify the participating departments and entities and clarify responsibilities. While defining responsibilities, the KCG shall identify a single entity and assign clear ownership or sponsorship of the project. This person/group will be responsible for making key decisions such as whether to increase the scope or budget of the project. The KCG shall agree on the procedure for handling changes that may arise during the development process as part of the determination of responsibilities.

4.2.5 Analysis and Design

The project team must undertake to review and analyse system requirements before system development work begins. The system requirements specification should describe: functions and capabilities of the system; organizational and user requirements; safety, security and

information privacy; operations and maintenance requirements; design constraints and qualification requirements.

A top-level architecture of the system must be established. The architecture should identify items of hardware, software/applications and manual operations. It should be ensured that all the system requirements are allocated among the items.

4.3 Acquisition

Application software, system software and application development software shall be acquired in consideration of information sharing, user satisfaction, compatibility, unified support, interoperability, scalability, quality and improved staff productivity. The KCG will be required to determine whether to develop software internally or externally, or procure vendor software.

4.3.1 Procurement

When procuring software, the KCG shall:

a. Ensure that there are no existing software applications within the KCG that provide equivalent functions and that can be replicated to avoid duplication.
b. Ensure that acquisition of the software is done in consultation and coordination with the head of the ICT department, who shall be responsible for the preparation and issuance of all technical specifications of the software.
c. Use requisition and acceptance forms to ensure that requests for procurement of software are validated by the head of the ICT department.
d. Ensure that requirements are clearly defined and documented when procuring enterprise software.
e. Ensure that only qualified ICT officers are allowed to install software.
f. Procure and use the latest versions of software.

4.3.2 In-house Development

When developing software in-house, the KCG shall:

a. Adopt a project management approach.
b. Ensure that an optimal system development methodology such as Software Development Life Cycle (SDLC) is adopted in order to obtain a useful system.
c. Constitute a development team consisting of various specializations as may be required for the specific software development task. These shall include software developers, system analysts, system designers, database experts, network and communication, security specialists and other skills that may be required in the project.
d. Establish and maintain an intellectual property agreement on software developed in-house.

4.3.3 Outsourced Development

For sophisticated systems development initiatives, the KCG may contract an external developer to deliver the application. The KCG shall consider the following tasks:

a. Define a strategy on how acquisition will be conducted.
b. Prepare a request for the supply of a product or service that includes the requirements.
c. Communicate the request for the supply of a product or service to potential suppliers.
d. Select one or more suppliers.
e. Develop an agreement with the supplier that includes acceptance criteria.
f. Identify necessary changes to the agreement.
g. Negotiate the agreement with the supplier.
h. Update the agreement with the supplier, as necessary.
i. Assess the execution of the agreement.
j. Provide data needed by the supplier and resolve issues in a timely manner.
k. Confirm that the delivered product or service complies with the agreement.
l. Provide payment or other agreed consideration.
m. Accept the product or service from the supplier, or other party, as directed by the agreement.
n. Ensure that the source code ownership is defined before engagement with the developer.
o. Close the agreement.

4.3.4 Commercial Off-The-Shelf Software

If the KCG decides to acquire a specific commercial off-the-shelf or open-source software solution, acquisition can be limited to:

a. Identifying the supplier.
b. Accepting or negotiating the conditions in a pre-defined license.
c. Lease or maintenance agreement.
d. Determining rights to intellectual property and data rights in the software system.
e. Agreeing on the price.

4.4 Development

The KCG shall take into consideration the following when acquiring application development software:

a. Type of application to be developed (i.e. desktop application, web-based application or server application).
b. Operating System (OS) 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. The speed of development.
g. Performance of the developed application.
h. Assistance in the enforcement of code.

i. Portability of the system to an operating system other than the one in which it was developed.
j. Fitness of the software for the application being developed.

4.4.1 Skills

The KCG shall ensure that ICT officers responsible for development of software are adequately trained on all application software acquired.

4.4.2 Documentation

The KCG shall ensure that all systems have the following documentation:

a. Project initiation documentation detailing the business case.
b. Feasibility study detailing the proposed solution.
c. Detailed user and technical requirements.
d. High level and detailed system design documents.
e. Evidence of user and technical training.
f. User and technical manuals.
g. Certificate of completion.

4.4.3 Security

Software security is characterized by objective evidence that all systems have sufficient protection against intentional subversion or forced failure due to the software architecture, design or construction of the code. In order to meet these criteria, the KCG shall:

a. Ensure that all critical applications are manned by qualified ICT staff who have been accredited by ICT Authority (ICTA).
b. Define requirements for achieving software assurance characteristics.
c. Define and implement an approach for achieving the desired software assurance.
d. Continuously monitor the extent of achievement of the security requirements.
e. Specify and achieve a satisfactory level of the critical software assurance characteristics.
f. Ensure the software and application acquisition conforms to information security standards.

4.4.4 Testing

The project team must conduct testing in accordance with the requirements for the application. It must be ensured that the implementation of each application requirement is tested for compliance. For each requirement of the system, a set of tests, test cases and test procedures for conducting system testing must be developed and documented. The project team must ensure that the integrated system is ready for system testing.

4.5 Maintenance

Application and system software shall be maintained regularly to ensure availability of service and operational continuity. The KCG must keep an inventory of all software and

generate annual reports on the status of integration and utilization, availability, performance, support and adaptability.

4.5.1 Change Management

The KCG shall establish standards and procedures for changes to application software in conformance with these standards. Participation of users should be facilitated in appropriate stages of the change process. The KCG should also ensure that all changes are documented, dated and retained.

If changes to software are required, the KCG shall determine:

a. The effect the change will have on the security controls in the software.
b. If consent of the vendor is required.
c. If the required functionality is included in a new version of the software.
d. If the KCG will become responsible for maintenance of the software as a result of the change.

4.5.2 Licences

Different applications and systems are implemented with varying licensing models. The KCG should ensure that appropriate software licences are provided upon acquisition, duly registered and subsequently renewed to ensure compliance. Service level agreements (SLAs) should also be signed with the vendors.

4.5.3 Updates

Software updates are important to ensure that vendor support is maintained, and that the latest performance and security patches are applied. The KCG shall ensure that all software is kept up-to-date.

4.5.4 Support

Wherever possible, software maintenance should be done in-house by ICT officers who shall develop maintenance schedules on upgrading and debugging. The head of the ICT department should prepare an annual maintenance report and forward it to the accounting officer. Sub-contracting for software maintenance shall be through appropriate justification and approval by the accounting officer after due diligence.

4.5.5 Security Audit

The KCG shall ensure that all software and applications are audited annually to ensure they conform with information security standards.

4.5.6 Training and Knowledge Transfer

The KCG shall ensure that ICT officers mandated to maintain or support software are adequately trained. Where a maintenance contract is in place, the KCG 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 on expiry of the contract.

4.6 Disposal

The purpose of the disposal process is to end the existence of a system or system element for a specified use, appropriately handle replaced or retired elements, and to properly attend to identified critical disposal needs (e.g. for environmental, legal, safety or security aspects). The KCG shall develop and maintain a policy to guide disposal of software in consideration of information security standards.

In preparation for disposal, the KCG shall define a disposal strategy for the software system to include each system element and to identify and address critical disposal needs, including the following considerations:

a. Permanent termination of the system's functions and delivery of services (e.g. physical destruction of data storage devices) or transition of the system elements for future reuse in modified or adapted form.
b. Identification of ownership and responsibility for retention or destruction of data and intellectual property in the software system.
c. Transformation of the product data, or retention in a socially and physically acceptable state, thereby avoiding subsequent adverse effects on stakeholders and the environment.
d. The health, safety, security and privacy concerns applicable to disposal actions and to the long-term condition of resulting physical material and information.
e. Notification of relevant stakeholders of significant disposal activities e.g. retirement or replacement of a system, software products or services, retirement schedule or replacement options.
f. Identification of schedules, actions, responsibilities and resources for disposal activities.

In performing the disposal of software, the KCG shall consider the following:

a. Deactivate the software system or element or prepare if for removal.
b. Remove the software system, its elements, data and non-reusable material from use or production for appropriate disposition and action.
c. Withdraw impacted operating staff from the software system or system element and record relevant operating knowledge.
d. Reuse, recycle, recondition, overhaul, archive or destroy designated system elements.
e. Conduct destruction of the system elements, as necessary, to reduce the amount of waste treatment or to make the waste easier to handle.
f. Confirm that detrimental health, safety, security and environmental conditions following disposal have been identified and treated.
g. Return the environment to its original state or to a state that is specified by agreement.
h. Archive information gathered through the lifetime of the product to permit audits and reviews to permit future system software creators and users to build a knowledge base from experience.

5 Messaging and Collaboration

5.1 Introduction

Communication is one of the most critical functions in an ICT infrastructure and the availability of effective messaging and collaboration tools affects organizations as a whole. Use of messaging and collaboration tools will encourage KCG to engage with stakeholders to share information and help promote the County Government's goals and vision in an efficient and effective way.

This standard offers guidance on how communication is carried out between KCG and various stakeholders with a view of making it more convenient and efficient.

5.2 General Requirements

Messaging and collaboration systems shall conform to the following as per the standards:

a. Ease of use
b. Agility
c. Scalability
d. Adaptable contexts
e. Support

5.3 Email

The KCG shall acquire and ensure appropriate use and management of email applications for official communications in accordance with the application software standard. The KCG shall ensure that the corporate email software solutions acquired provide for:

a. Sending of group emails.
b. Creation of mailing lists.
c. Email search and retrieval.
d. Creation of email folders.
e. Email archival.
f. Global address book for all registered users.
g. Sending email attachments.
h. Appending of a digital signature.
i. Email autoresponder.
j. Formatting of email messages (text and graphics).
k. Email account management.
l. Security: spam and junk mail filtering, password management and client/server system patching.
m. Adequate disk quota for all users.
n. Backup of user mailboxes.
o. Push notification support for mobile devices.
p. Firewall and antivirus protection for the email server.
q. Transmission of email messages using encryption technologies.

5.4 Audio and Video Conferencing

The KCG shall ensure appropriate acquisition, management and use of video and audio-conferencing applications. When a video and audio-conferencing software is required, the VoIP software acquired must provide for:

a. Traditional calling features, including call by name, caller ID, last number redial, hold, call waiting, call forwarding, transfer, divert, park, retrieve, voicemail, return call and call conferencing.
b. User-controlled delegation to ensure calls can be answered by administrative assistants.
c. Team calling.
d. Telephone directory.
e. Maintaining call history.
f. Local number portability, that is, ability to phone numbers when changing service providers.
g. End-to-end encryption where possible.

5.5 Social Media

The KCG shall ensure appropriate use and management of social media applications by establishing and maintaining a social media policy and create awareness of the policy to its staff.

The KCG shall put in place appropriate mechanisms to manage the presence of the County Government and affiliated departments on social media networks/platforms. Rules of engagement on social media shall also be developed and disseminated.

6 Networks

6.1 Introduction

ICT networks create new ways to work and increase productivity by making it easy and fast to share information. Networks enable more efficient use of resources, permitting communication and collaboration across distance and time.

This standard establishes guidelines for planning, design, implementation, utilization and management of network infrastructure by the KCG with a view to:

i. Provide shared infrastructure services.
ii. Provide a platform for shared services.
iii. Facilitate data, multimedia and voice communication.
iv. Reduce infrastructure development and management costs.
v. Remove/manage duplication.
vi. Enable integration of future technologies.
vii. Enable real time backup and disaster recovery services.
viii. Provide a comprehensive security solution.
ix. Facilitate conformity to international standards.

6.2 Definitions

Local Area Network (LAN)

A LAN is a computer network that is confined to a relatively small area, such as a building. A LAN allows computers to access and share data and devices such as printers. Devices on a LAN can be connected using cables or wirelessly (wireless LAN or WLAN).

Wide Area Network (WAN)

A WAN is a telecommunications network that exists over a large geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metropolitan area networks (MANs). This ensures that computers and users in one location can communicate with computers and users in other locations.

Virtual Local Area Network (VLAN)

A VLAN is a subnetwork which can group together collections of devices on separate physical LANs and allow them to communicate in a simulated environment as if they exist in a single LAN.

Virtual Private Network (VPN)

A VPN is a network that is built over public infrastructure to allow access to a private/internal network from different locations via a public network, usually the Internet. The VPN is secured using encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Network Address Translation (NAT)

NAT is a process in which private IP addresses for devices in a LAN are translated into one or more public/global IP addresses and vice versa in order to provide Internet access to devices on the LAN.

6.3 Telecommunication Rooms, Pathways and Spaces

The KCG shall ensure telecommunication rooms, pathways and spaces are properly designed and adaptable to change.

Telecommunication rooms should be of sufficient size to handle the cross connect field, associated electronic equipment, cabling and pathways. The telecommunication/equipment rooms should be neatly organized and well ventilated, with room for working access to cabinets in all directions. Telecommunications rooms should be located in secure areas and fitted with access control measures and CCTV surveillance in accordance with information security standards.

6.4 Network Design, Configuration, Documentation and Commissioning

a. The KCG shall carry out site surveys to ensure a network design that guarantees maximum service availability.
b. The KCG shall develop a network design with associated specifications and Bill of Quantities (BoQ).
c. The KCG shall ensure that relevant functionalities are installed and configured to deliver a robust and secure IP network.
d. Upon completion of the installation and configuration of the network, the KCG shall carry out tests and record the results in one or several measure books showing test results of the cable components.
e. The KCG shall ensure that physical and logical design of the network is documented as built. The documentation shall also include: synopsis of the cabling (primary and secondary), charts of the distribution highlighting the details of the elements that have been installed, detailed map of socket layout and reports on measurements.
f. All components shall be tested and a completion certificate issued.
g. Physical and logical designs shall be updated whenever changes occur.

6.5 Network Monitoring and Management

a. The KCG shall acquire an appropriate monitoring and management tool/software. The tool shall have capability to: discover network components such as devices and links, generate a layout of the existing network, report failures and event logs, and generate customized reports.
b. The KCG shall ensure that network monitoring and management roles are defined.
c. The KCG shall ensure that usage and utilization of bandwidth is controlled using appropriate bandwidth management tools, or traffic/packet shapers.

d. A VLAN shall be dedicated for management purposes and shall not be used to forward traffic externally. Remote access shall be through a Virtual Private Network (VPN) and network address translation (NAT) functionality which must be enabled.
e. The KCG shall ensure Service Level Agreement (SLA) are maintained with a minimum of LAN, WAN and Internet service availability of 99.99%.
f. The KCG shall specify the mean time to failure for all replaceable devices using acceptable methods for predicting the failure for electronic equipment.

6.6 Preventive Maintenance

a. Maintenance programs shall be identified to detect imminent or conditional failures such as thresholds for CPU and memory, interface utilisation and errors, temperature, power supply current and voltage.
b. Maintenance programs shall be identified for all assets to ensure that the hardware, firmware, software, physical and logical configuration is as designed throughout the life of the asset.

6.7 Wireless Network Connectivity

a. Wireless network installation shall be authenticated between wireless clients and access points to ensure that clients do not connect to a rogue access point deployed by an attacker. This would also ensure that unauthorized wireless users do not connect to the KCG wireless networks.
b. Sensitive data between wireless clients and access points should be protected using encryption.
c. Use of network ID (SSID) and enforcement of MAC address filtering shall be used to secure wireless networks.
d. WPA2 shall be used as bare minimum security for authentication and protection of information on a wireless LAN (WLAN).
e. The KCG shall change the keys/secrets associated with the wireless access points regularly through a managed process.
f. The KCG shall periodically scan for unauthorised wireless access points and take appropriate action if such access points are discovered. The scan should not be limited to only those areas containing the high-impact information systems, but should also cover the adjacent areas.
g. The KCG may create guest VLANs for guests to access the Internet only.
h. Wireless networks should be reviewed from time to time to ensure that obsolete networks are retired and up-to-date networks installed that meet the performance requirements.

6.8 Internet

a. The KCG shall ensure that Internet bandwidth is adequate for the needs of its users.
b. Internet service availability shall be at least 99.99%.
c. The KCG shall sign and enforce a Service Level Agreement (SLA) with the Internet Service Provider (ISP) to guarantee 99.99% availability.

d. The KCG shall assign internal workstation network IP addresses using Dynamic Host Configuration Protocol (DHCP).
e. The KCG shall use subnetting to protect IPv4 spaces as may be applicable.
f. The KCG shall ensure redundancy for Internet connectivity for high availability.
g. The KCG shall develop and sensitize users on acceptable Internet usage policy.
h. The KCG shall ensure that new county government buildings and offices are Internet ready.

6.9 Network Security

The KCG shall ensure the following are configured in line with information security standards:

a. VLANs - Firewall and Perimeter Security Architecture.
b. Connections to third parties.
c. Remote network administration to servers.
d. Encryption of sensitive information.
e. Antivirus protection.
f. Email security.
g. Wireless security management.
h. Redundancy of network infrastructure.
i. Auditing and monitoring of security logs.
j. Network intrusion detection - network segmentation.
k. Segregation of duties.
l. Default user IDs and network device configuration.
m. Network inventory and asset management.
n. Network configuration management.
o. Vulnerability and patch maintenance.

7 Cloud Computing

7.1 Introduction

Cloud computing is the delivery of resources such as networks, servers, storage and applications through the Internet. The goal of cloud computing is to provide simple, on-demand access to IT resources and services. It offers users and organizations a viable alternative to costly information management technology and infrastructure by outsourcing it to third-party providers.

There are several characteristics of cloud computing:

i. **Scalable**: Cloud infrastructure is able to handle growing workload requirements while maintaining consistent performance.
ii. **Elastic**: Cloud services can be scaled up and down dynamically as needed to adapt to workload changes in an automatic manner, maximizing the use of resources.
iii. **Self-service**: The process of adding capacity can be done by users with a simple request via web portals with very short lead times.
iv. **Ubiquitous access**: All capabilities can be accessed from anywhere using any device.
v. **Measured service**: Most cloud services have the ability to bill for precisely the amount of resources consumed, with no prior commitment.
vi. **Multiple tenants**: Shared computing resources are often used to provide cloud services to multiple customers, offering greater utilization rates. Virtualization is used to separate and protect each customer's data, making it appear as though they are the only users of the shared resources.

This standard outlines the various considerations for the Kisii County Government in the selection and deployment of cloud computing services.

7.2 Definitions

Private Cloud

Private cloud is a model of cloud computing for the provision of ICT services for the dedicated use of a single organization with completely isolated access. A private cloud can be owned by the organization or rented from a third-party provider as part of a managed private cloud approach. With complete ownership, the organization is responsible for staffing, managing and maintaining all underlying infrastructure.

Public Cloud

Public cloud is a model of cloud computing used for the provisioning of ICT services to the general public over the internet. A public cloud is owned and managed by a third-party company and automatically provisioned and allocated among multiple clients through a self-service interface. The provider maintains the hardware underneath the cloud, supports the network and manages the virtualization software.

Community Cloud

A community cloud is a hybrid form of private cloud that is built and operated specifically for a targeted group of organizations sharing the same concerns or needs. It may be managed by one or more of the organizations or a third party and may exist on premise or off premise.

Hybrid Cloud

A hybrid cloud incorporates two or more cloud deployment models to handle the mixed needs of an organization. The presence of multiple environments allows an organization to minimize data exposure by moving workloads and data across environments based on compliance, audit, policy or security requirements.

Software as a Service (SaaS)

SaaS is a form of cloud computing that delivers an application to users over the Internet. Users interact with the application through a web browser or application programming interface (API). Typically, a cloud service provider manages the application and takes care of software updates, bug fixes, and other general software maintenance. The provider is also responsible for the underlying hardware components (e.g. networking, storage and servers) and platform (e.g. operating system and middleware).

Platform as a Service (PaaS)

PaaS is a form of cloud computing where a software development environment is provided to users, primarily developers and programmers. PaaS allows users to develop, run and manage their own applications without having to build and maintain the infrastructure or platform associated with the process. A PaaS provider hosts the hardware and software on its own infrastructure and delivers this platform to the user as an integrated service through an internet connection.

Infrastructure as a Service (IaaS)

IaaS is a form of cloud computing in which resources required to operate and manage IT environments are provided to users through the Internet. In this model, users handle the applications, data, operating system, and middleware, while the vendor provides storage, network and servers. In most cases, the user is given control of the infrastructure through an application programming interface (API).

7.3 General Requirements

a. Use of cloud computing services must comply with all current laws, information security standards, and risk management policies.

b. The KCG shall not host critical applications in the public cloud.

c. To mitigate against risks associated with vendor lock-in, the KCG shall prepare an exit strategy as part of contracting with the cloud service provider.

d. The KCG shall obtain copies of potential cloud service providers' most recent standards-based security assessment/assurance as early in the procurement cycle as possible.

e. Cloud solutions that store personally identifiable citizen data shall be within the boundaries of Kenya.

f. The KCG shall determine licensing needs projected over a period and ensure the cloud provider meets the needs.

g. Any data on foreigners handled by the KCG shall ensure compliance to applicable laws of their countries of origin.

h. If data stored with a cloud service provider is to be encrypted this shall be done using cryptographic keys owned and managed by the KCG.

i. In all cases, a cloud computing solution shall only be considered after a thorough risk evaluation has been completed, reviewed and accepted by the KCG.

j. The KCG shall ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions.

k. The KCG shall acquire cloud solutions in reference to the list of accredited cloud providers provided by ICT Authority.

l. Contracts with cloud service providers shall include:

   i. An exit plan with a requirement for the cloud provider to provide a way for the KCG to extract data easily and economically.

   ii. Requirement for data sanitization from storage media, electronic and physical access rights be revoked from the cloud provider, and assets provided to the provider returned or, if not possible, be securely purged.

   iii. Non-disclosure agreements (recommended before provisioning any service).

   iv. Full disclosure in case of breaches to regulated information.

   v. Data ownership (the KCG retains exclusive ownership of all data held in a cloud provider's solution which was entered by the KCG or affiliates in all media forms e.g. online, backup and archive etc.)

   vi. Any other standard intellectual property clauses (as are relevant to the service).

   vii. Data location (it should be explicitly stated in contracts that it should be in Kenya).

   viii. Privacy legislation compliance.

ix. Service level agreements (to meet availability, performance, and disaster recovery requirements).

x. Service management processes.

xi. Procedures for incident response and ensure that they meet the requirements of the KCG.

xii. Audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

xiii. The application of appropriate retention policies to store data based on its classification (this means the cloud service provider's solution must not hinder compliance with the Public Records Act).

xiv. A clear process documenting the responsibilities of each party with respect to extracting the KCG's data and destroying data at the end of the contract.

xv. Provision for a cloud service provider being taken over/bought-out by another organisation (this should include ensuring the ownership, access rights and protection of any data the KCG owns cannot be lost when there is a change of cloud service provider ownership).

7.4 Auditability

a. The KCG shall ensure that cloud services are independently audited for assurance that those services are provided and used in consistency with the associated service agreements between the KCG, cloud service providers and cloud service partners.
b. The KCG shall ensure that governing agreements guarantee availability and security of data and evidence including records and logs of activities and conditions of the operational environments of all parties. This is necessary for the audit of the usage, environment, availability and performance of cloud services and associated resources.

7.5 Interoperability

a. The KCG shall ensure that interaction with the cloud service and exchange of information is done according to a prescribed method and that predictable results can be obtained as per the agreed specification, one that is possibly standardized.
b. The KCG shall be able to use widely available ICT facilities in-house when interacting with cloud services, avoiding the need to use proprietary or highly specialized software.
c. The KCG shall have a consistent and interoperable interface to the cloud service management functionality and be able to interact with two or more cloud service providers without needing to deal with each provider in a specialized way.
d. The cloud service implementations shall support the evolution of the standards used, both from an earlier version of a standard to a later version, or from one standard to a different one, while minimizing disruptive changes.

7.6 Maintenance and Versioning

a. Maintenance of cloud services shall be subject to governance practices that are transparent to the KCG.
b. Maintenance shall be documented in the SLA for the cloud services and shall include the capability for the customer to report problems and request fixes and also a mechanism for the cloud service provider to notify the customer of pending maintenance changes and their schedule.
c. The KCG shall ensure that appropriate labelling of a service is done to identify the version (or of components of a service, such as the operating system level used in an IaaS service), so that it is clear that a particular version is in use. The service shall be given a new version label when maintenance of a cloud service occurs.
d. Where significant changes are made to a service between two versions, the older version of the service shall be available in parallel with the new versions for an agreed period of time.

7.7 Performance

The KCG shall ensure that metrics for performance are defined in the SLA for each performance condition identified and these metrics shall be monitored during operation of the cloud service to ensure that the service meets the performance terms of the SLA. The metrics shall include:

a. Availability of the service.
b. Response time to complete service requests.
c. Transaction rate at which service requests are executed.
d. Latency for service requests.
e. Data throughput rate (input and output).
f. Number of concurrent service requests (scalability).
g. Capacity of data storage.
h. The number of concurrent execution threads available to an application (for IaaS and PaaS).
i. The amount of memory (RAM) available to the running program (for IaaS and PaaS).
j. Data centre network IP address pool and/or VLAN range capacity.

7.8 Portability

The KCG shall ensure that lock-in is avoided when they choose to use cloud services. They shall ensure that they can move cloud service customer data or their applications between multiple cloud service providers at low cost and with minimal disruption.

a. **Cloud data portability**: The KCG shall be able to copy its data into or out of a cloud service through network access or by physical transfer of storage devices.
b. **Cloud application portability**: Could services shall allow the migration of items such as a fully-stopped virtual machine instance or a machine image (IaaS service) from one cloud service provider to another cloud service provider, or the migration of application components (PaaS service) from one cloud service provider to another. In

both cases, there is a related aspect of the support of portability of metadata relating to the application components, providing information about the relationships of program components and about the required infrastructure for the program components (e.g. load balancing configuration, firewall settings).

7.9 Protection of Personally Identifiable Information

a. The KCG shall ensure the protection, assurance, proper and consistent collection, processing, communication, use and disposition of personally identifiable information (PII) in relation to cloud services.
b. The KCG shall ensure adherence of cloud services to statutory, regulatory and legal requirements rules and regulations applied to the handling of PII.

7.10 Resilience

The KCG shall implement a set of monitoring, preventive and responsive processes to enable a cloud service to provide continuous operations, or predictable and verifiable outages, through failure and recovery actions. These can include hardware, communication and/or software failures, and can occur as isolated incidents or in combination, including serial failure. These processes can include both automated and manual actions, usually spanning multiple systems, and thus their description and realization are part of the overall cloud infrastructure, not an independent function.

7.11 Reversibility

a. The KCG shall put in place measures to retrieve their data and application artefacts and for the cloud service provider to delete all their data, as well as contractually specified cloud service derived data after an agreed period.
b. The cloud service provider shall ensure the "right to be forgotten" is implemented, in that once they indicate to the cloud service provider that their use of the service(s) will cease, there will be an orderly process for the cloud service customer to retrieve their data and their application artefacts and that the cloud service provider will delete all copies and not retain any materials belonging to them after an agreed period.

7.12 Security

a. The KCG shall implement security capabilities for cloud services including those for access control, confidentiality, integrity and availability.
b. The KCG shall implement facilities to enable early detection, diagnosis and fixing of cloud service and resource related problems; secure logging of access records, activity reports, session monitoring and packet inspections on the network; provision of firewalling, and malicious attack detection and prevention for the cloud service providers' systems. One user should not be able to disrupt other users' use of cloud services.
c. Intranet level security shall be provided on the network connecting the KCG to the cloud service provider (for example, through the use of VPN capabilities).

d. The KCG shall ensure a clear definition of the information security responsibilities between them and the provider to ensure that all aspects of security are covered, to avoid responsibility ambiguity.
e. The KCG shall implement security measures that address the threats affecting the specific cloud service category i.e. IaaS, PaaS, SaaS.
f. The KCG shall implement security measures that address the threats affecting the specific cloud deployment models.
g. The KCG shall properly catalogue its data and identify its sensitivity and the risk to the county government of its leakage, loss or corruption.
h. In case of encryption, the KCG shall ensure the responsibility for key management is clearly defined and the logical and physical control of the keys, as well as the data are implemented.

7.13 Service Level Agreements

a. The KCG shall ensure service level agreements are in place to assure an agreed upon quality of service with cloud service providers.
b. The K shall cover terms regarding the quality of service, security, performance and remedies for failures to meet the terms of the SLA.
c. The SLA shall list a set of promises explicitly not made to the KCG, i.e., limitations and obligations that cloud service customers need to accept.
d. The cloud SLA shall define the classification of data objects (i.e. cloud service customer data, cloud service provider data, and cloud service derived data), who has access and control of data objects in these data classifications and how they will be used.
e. The service level agreement shall specify information relating to the availability of the services, the confidentiality and integrity of the services and the access controls which apply to the services. The service level agreement shall specify how any personally identifiable information will be handled in relation to the cloud services.
f. The KCG shall review the service agreement – alternatively known as the master service agreement (MSA), terms of service (ToS), terms and conditions (T&C), or simply "the contract" – (which is the higher order document in agreements between parties and the service level agreement (SLA) is subservient) to ensure they are aligned.

8 Information Security

8.1 Introduction

Data and information are assets that are essential to the KCG and its operations, and consequently need to be suitably protected in order to ensure information confidentiality, integrity and availability.

Information security is characterized by the following elements:

i. **Confidentiality**: Ensuring that information is only accessible to those with authorized access.

ii. **Integrity**: Safeguarding the accuracy and completeness of information and processing methods.

iii. **Availability**: Ensuring that authorized users have access to information when required.

iv. **Compliant use**: Ensuring that the KCG meets all legal and contractual obligations.

v. **Responsible use**: Ensuring that appropriate controls are in place so that users have access to accurate, relevant and timely information, but that they do not adversely affect other users or systems.

This standard aims to guide the KCG in setting up appropriate controls that will ensure the protection of information from a wide range of threats in order to ensure continuity of operations, minimize risk and maximize return on ICT investments. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific ICT security and operational objectives of the KCG are met.

8.2 Cybersecurity Management

Cybersecurity management is characterized by actions undertaken by the KCG to protect its information systems and computer networks from cyberattacks, intrusion, malware and various types of data breaches.

8.2.1 Mobile Device Management

a. The KCG shall put in place protection measures to avoid unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques and enforcing the use of secret authentication information.

b. Administrator level accounts shall only be used by authorized ICT administrators and all other users shall be limited to basic accounts.

c. Devices carrying important, sensitive or critical information shall not be left unattended, and shall be physically locked away where possible, or special locks shall be used to secure the devices.

d. The KCG shall have a special procedure taking into account legal, insurance and other security requirements of the KCG for cases of theft or loss of mobile devices.

e. The KCG shall arrange training for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and controls that should be implemented.

8.2.2 Teleworking

Teleworking involves use of communication tools to carry out work duties from a remote location.

To allow a secure teleworking environment, the KCG shall:

a. Identify the roles/jobs which may be considered for teleworking.

b. Identify the types of networks and applications which may be provided to teleworkers.

c. Identify the classified information types that should not be made available to teleworkers.

d. Ensure teleworkers are identified, authenticated and authorized before accessing KCG resources.

e. Ensure specific equipment or software products required to facilitate teleworking are deployed on the teleworker's PC.

f. Ensure the teleworker's PC configuration is protected, updated and monitored.

g. Ensure the user understands their role in protecting KCG resources, e.g. appropriate use of resources, use of antivirus software, and use of encryption tools.

h. Ensure the user understands the possible information risks associated with teleworking, how those risks are addressed, and the user's role in minimizing the risks.

i. Ensure that a code of practice is signed by teleworkers for accountability.

8.2.3 Malware Defence

a. The KCG shall utilize centrally managed anti-malware software to continuously monitor and defend all workstations and servers.

b. The KCG shall ensure that anti-malware software receives regular updates to its scanning engine and signature database.

c. The KCG shall configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

d. The KCG shall configure devices not to auto-run content from removable media.

e. The KCG shall send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.

8.2.4 Administrative Privileges

a. The KCG shall enforce strong password policies for administrator accounts.

b. The KCG shall use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

c. The KCG shall change all default passwords before deploying any new asset to have values consistent with administrative level accounts.

d. The KCG shall ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not daily user activities.

e. Multi-factor authentication and encrypted channels shall be used for all administrative account access.

f. Where multi-factor authentication is not supported, accounts will use passwords that are unique to that system.

g. The KCG shall limit access to scripting tools to only administrative or development users with the need to access those capabilities.

h. The KCG shall configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

i. The KCG shall configure systems to issue log entries and alerts on unsuccessful logins to an administrative account.

8.3 Systems and Applications Security

8.3.1 Systems Acquisition and Development

a. The KCG shall ensure vendor supplied defaults for system passwords and other security parameters are changed.

b. The KCG shall ensure secure coding practices appropriate to the programming language and development environment are being used.

c. The KCG shall ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

d. The KCG shall verify that the version of all software acquired from external parties is still supported by the developer or appropriately hardened based on developer security recommendations.

e. The KCG shall use up-to-date and trusted third-party components for the software developed in-house.

f. The KCG shall only use standardized and extensively reviewed encryption algorithms for security sensitive information e.g. database hashes for passwords.

g. The KCG shall ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities to reduce dependency on contractors.

h. The KCG shall apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.

i. The KCG shall establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact the information security group.

j. The KCG shall maintain separate environments for production and non-production systems.

k. The KCG shall protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

l. The KCG shall use standard hardening configuration templates for systems as applicable e.g. web, DNS, mail servers.

m. In the event the system is not fully owned by the KCG, escrow agreements shall be entered with third parties to safeguard of source code.

n. For both in house and off shelf systems, the KCG shall require that quality assurance is guaranteed in meeting the requirements of the system.

o. The KCG shall ensure user acceptance testing is performed before acceptance of the system.

p. The KCG shall ensure proper error handling is performed to only give the required output and not give out excessive information on backend technologies.

8.4 Communication Security

8.4.1 Network Security

a. The KCG shall maintain an up-to-date inventory of all of the network perimeters.

b. The KCG shall perform regular scans from outside each trusted network perimeter to detect any unauthorized connections which are accessible across the network boundary.

c. The KCG shall deny communications with known malicious Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the network boundaries.

d. The KCG shall deny communication over unauthorized ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the network boundaries.

e. The KCG shall deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the network boundaries.

f. The KCG shall deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the network boundaries.

g. The KCG shall enable the collection and monitoring of network flows and data logging on network boundary devices.

h. The KCG shall ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.

i. The KCG shall decrypt all encrypted network traffic at the boundary proxy prior to analysing the content. However, whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic may be employed.

j. The KCG shall require all remote login access to the network to encrypt data in transit and use multi-factor authentication.

k. The KCG shall maintain standard, documented security configuration standards for all authorized network devices.

l. The KCG shall configure rules that allow traffic to flow through network devices and should be documented in a configuration management system with a specific operational reason for each rule.

m. The KCG shall compare all network device configurations against approved security configurations defined for each network device in use and alert when any deviations are discovered.

n. The KCG shall install the latest stable version of any security related updates on all network devices.

o. The KCG shall manage network devices using multi-factor authentication and encrypted sessions where possible.

p. The KCG shall separate networks through VLANs or, preferably, on entirely different physical connectivity for different network segments.

q. The KCG shall associate active ports, services and protocols to the hardware assets in the asset inventory.

r. The KCG shall ensure that only network ports, protocols, and services listening on a system with validated operational needs are running on each system.

s. The KCG shall perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

t. The KCG shall apply host-based firewalls or port filtering tools on end systems, with a default deny rule that drops all traffic except those services and ports that are explicitly allowed.

u. The KCG shall place application layer firewalls in front of any critical network segments to verify and validate the traffic going to the network. Any unauthorized traffic should be blocked and logged.

8.4.2 Wireless Security

a. The KCG shall maintain an inventory of authorized wireless access points connected to the wired network.

b. The KCG shall configure network vulnerability scanning tools to monitor, detect and alert on unauthorized wireless access points connected to the wired network.

c. The KCG shall disable wireless access on devices that do not have an operational purpose for wireless access or pose a risk in facilitating adhoc wireless connections (computer to computer), by-passing network controls.

d. The KCG shall leverage wireless encryption standards for data in transit.

e. The KCG shall ensure that wireless networks use authentication protocols that require multi-factor authentication.

f. The KCG shall create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

g. The KCG shall can wireless devices for malware before admission to the network.

8.4.3 Electronic Messaging

a. The KCG shall protect messages from unauthorised access, modification or denial of service.

b. The KCG shall ensure correct addressing and transporting of electronic messages.

c. The KCG shall require electronic signatures for all messages.

d. The KCG shall ensure approval is obtained prior to using public services such as instant messaging, social media or file sharing.

e. The KCG shall implement cryptographic technologies to protect user authentication and email data.

f. The KCG shall ensure that messaging clients are deployed, configured and used properly to meet security requirements.

8.4.4 Information Sharing

The KCG shall develop formal transfer policies, procedures and controls to protect the transfer of information through the use of communication facilities. The following shall be considered:

a. Procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction.

b. Procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications.

c. Procedures for protecting communicated sensitive electronic information that is in the form of an attachment.

d. Policies or guidelines outlining acceptable use of communication facilities.

e. Personnel, external party and any other user's responsibilities not to compromise the KCG, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.

f. Use of cryptographic techniques to protect the confidentiality, integrity and authenticity of information.

g. Retention and disposal guidelines for all official correspondence, including messages, in accordance with relevant legislation and regulations.

h. Controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses.

i. Advising personnel to take appropriate precautions not to reveal confidential information.

8.4.5 Information Transfer

The KCG shall be subject to terms of agreement to address the secure transfer of information between the KCG and external parties. The information security content of the agreement shall reflect the sensitivity of the information involved.

The information transfer agreements should incorporate the following:

a. Management responsibilities for controlling and notifying transmission, dispatch and receipt.

b. Procedures to ensure traceability and non-repudiation.

c. Minimum technical standards for packaging and transmission.

d. Courier identification standards.

e. Responsibilities and liabilities in the event of information security incidents, such as loss of data.

f. Use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected.

g. Technical standards for recording and reading information and software.

h. Any special controls that are required to protect sensitive items, such as cryptography.

i. Maintaining a chain of custody for information while in transit.

j. Acceptable levels of access control.

8.5 Risk Management

8.5.1 Information Asset Management

a. The KCG shall implement and maintain an inventory of assets associated with information and information processing facilities.

b. For each of the identified assets, ownership of the asset shall be assigned and the classification shall be identified.

c. The owner shall ensure the assets are appropriately classified and protected.

d. The KCG shall ensure labelling of classified information. Physical labels and metadata shall be used.

e. The owner shall define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;

f. The owner shall ensure proper security of information when the asset is retired or destroyed.

g. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, created, documented and implemented.

h. Staff and external parties using or having access to the KCG assets shall be made aware of the information security requirements of the assets associated with information and information processing facilities and resources.

i. Use of messaging and collaboration, social media, BYOD shall conform to the systems and applications standard.

j. All staff and external parties shall return all of the KCG assets in their possession upon termination of their employment, contract or agreement unless there exists an arrangement for transfer of ownership.

k. The termination process shall be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the user by the KCG.

l. In cases where an employee or external party has knowledge that is important to ongoing operations, that information shall be documented and transferred to the KCG.

m. During the notice period of termination, the KCG shall control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

n. The KCG shall develop and implement a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

o. The clear desk and clear screen policy shall take into account the information classifications, legal and contractual requirements and the corresponding risks and cultural aspects of the KCG. The following guidelines shall be implemented:

   i. Sensitive or critical information on paper or on electronic storage media, shall be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

   ii. Computers and terminals shall be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and shall be protected by key locks, passwords or other controls when not in use.

   iii. Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) shall be prevented.

p. The KCG shall ensure the physical asset is maintained in accordance with the supplier's recommended service intervals and only authorized maintenance personnel shall carry out repairs and service equipment.

q. Records shall be kept of all suspected or actual faults, and of all preventive and corrective maintenance.

r. Appropriate controls shall be implemented when the asset is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the KCG Where necessary, information shall be cleared from the asset or the maintenance personnel shall be cleared.

s. All maintenance requirements imposed by insurance policies shall be complied with.

t. Before putting the asset back into operation after its maintenance, it shall be inspected to ensure that it has not been tampered with and does not malfunction.

u. The KCG shall develop procedures for the management of removable media in accordance with the classification scheme adopted.

v. The KCG shall document formal procedures for the secure disposal of media and assets to minimize the risk of confidential information leakage to unauthorized persons. All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

8.5.2 Information Classification and Sharing

a. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification and aligned to the access control policy.

b. Each classification level shall be given a name that makes sense in the context of the classification scheme's application.

c. The scheme shall be consistent across the entire KCG so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.

d. Classification shall be included in the KCG processes, and be applied in a consistent and coherent way. Results of classification shall indicate value of assets depending on their sensitivity and criticality to the KCG. Results of classification shall be updated in accordance with changes of their value, sensitivity and criticality through their lifecycle.

e. The KCG shall ensure labelling of classified information using physical labels and metadata.

f. The KCG shall ensure access restrictions supporting the protection requirements for each level of classification.

g. The KCG shall ensure maintenance of a formal record of the authorized recipients of assets.

h. The KCG shall ensure protection of temporary or permanent copies of information to a level consistent with the protection of the original information.

i. The KCG shall ensure storage of IT assets in accordance with manufacturers' specifications.

j. The KCG shall ensure clear marking of all copies of media for the attention of the authorized recipient.

k. The KCG shall document and implement the following guidelines to protect media containing information being transported:

   i. Reliable transport or couriers shall be used.

   ii. A list of authorized couriers shall be agreed with management.

   iii. Procedures to verify the identification of couriers shall be developed.

   iv. Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturer's specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.

   v. Logs shall be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

8.5.3 Information Backup

a. The KCG shall keep accurate and complete records of backup copies and documented restoration procedures.

b. The backups shall be stored in a remote location, at a sufficient distance to escape any physical damage from a disaster at the main site.

c. Backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site.

d. Backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary. This shall be combined with a test of the restoration procedures and checked against the restoration time required.

e. Testing the ability to restore backed-up data shall be performed on dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss.

f. In situations where confidentiality is of importance, backups shall be protected by means of encryption.

g. Operational procedures shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups.

h. Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans.

i. Backup arrangements should cover all systems information, applications and data of critical systems that are necessary to recover the complete system in the event of a disaster.

j. The retention period for essential operational information shall be determined, taking into account any requirement for archive copies to be permanently retained.

8.5.4 Business Continuity and Disaster Recovery Plan

The KCG shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

The KCG shall ensure that:

a. Adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence.

b. Incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated.

c. Documented plans, response and recovery procedures are developed and approved, detailing how the KCG will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

The KCG shall establish, document, implement and maintain:

a. Information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools.

b. Processes, procedures and implementation changes to maintain existing information security controls during an adverse situation.

c. Compensating controls for information security controls that cannot be maintained during an adverse situation.

d. Appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements.

8.5.5 Threat and Vulnerability Management

a. The KCG shall develop and maintain an effective management process for technical vulnerabilities.

b. The KCG shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required.

c. Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them shall be identified for software and other technology based on the asset inventory list.

d. Timelines shall be defined to react to notifications of potentially relevant technical vulnerabilities.

e. Once a potential technical vulnerability has been identified, the KCG should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls.

f. Patches shall be tested and evaluated before they are installed on a production system to ensure they are effective and do not result in side effects that cannot be tolerated. If no patch is available, other controls shall be considered, such as: turning off services or capabilities related to the vulnerability, adapting or adding access controls such as firewalls at network borders, increased monitoring to detect actual attacks or raising awareness of the vulnerability.

g. The technical vulnerability management process shall be regularly monitored and evaluated in order to ensure its effectiveness and efficiency.

h. An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur.

i. The KCG shall define a procedure to address the situation where vulnerability has been identified but there is no suitable countermeasure.

j. The KCG shall establish a formal policy prohibiting the use of unauthorized software and implement controls that prevent or detect the use of unauthorized software suspected malicious websites.

k. The KCG shall establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, and reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management.

l. Regular reviews of the software and data content of systems supporting critical business shall be conducted and the presence of any unapproved files or unauthorized amendments shall be formally investigated.

m. The KCG shall carry out installation and regular updates of anti-malware software.

n. Procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks shall be defined.

o. The KCG shall define and enforce strict policies on which types of software users may install, and identify and document what types of software installations are permitted and what types of installations are prohibited.

8.6 Human Resource Security

The KCG shall ensure that both staff and contractors understand their information security responsibilities and are suitable for the roles for which they are considered.

8.6.1 Background Screening

a. The KCG shall conduct background verification checks on all candidates for employment in accordance with relevant laws, regulations and ethics.

b. The screening shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

c. Internal promotions that involves the person accessing mission critical assets shall also attract further and more detailed vetting

d. The KCG shall have contractual agreements (code of conduct) with their employees and contractors that reflect the policies for information security.

8.6.2 In-Service

The KCG shall ensure that:

a. Al staff and contractors are provided with guidelines to state information security expectations of their role within the KCG.

b. All staff and contractors conform to the terms and conditions of employment, which includes information security policies and appropriate methods of working.

c. All staff and contractors are provided with an anonymous reporting channel to report violations of information security policies or procedures (whistle blowing).

d. There is a formal and communicated disciplinary process in place to take action against staff who have committed an information security breach.

8.6.3 Termination or Change of Responsibilities

a. The KCG shall communicate termination or change of responsibilities appropriately to all relevant functions.

b. All access rights issued shall be disabled or reassigned in accordance with the access control policy.

8.6.4 Information Security Awareness

a. The KCG shall conduct an information security awareness programme in line with information security policies and relevant procedures, taking into consideration the information to be protected and the controls that have been implemented to protect the information.

b. The awareness programme shall include a number of awareness-raising activities such as public campaigns (e.g. an information security day) and issuing booklets or newsletters.

c. The awareness programme shall be planned taking into consideration the employees' roles in the KCG, and, where relevant, the KCG's expectation of the awareness of contractors.

d. Information security education and training shall take place annually. Initial education and training apply to those who transfer to new positions or roles with substantially different information security requirements, not just to new staff and should take place before the role becomes active.

e. An assessment of the employees' understanding shall be conducted at the end of an awareness, education and training course to test knowledge retention and understanding.

8.7 Operational Control

The KCG shall ensure correct and secure operations of information processing facilities.

8.7.1 User Access Management

8.7.1.1 User Registration and De-registration

The KCG shall develop a formal user registration and de-registration process to enable assignment of access rights. The process for managing user IDs should include:

a. Using unique user IDs to enable users to be linked to and held responsible for their actions. The use of shared IDs should only be permitted where they are necessary for operational reasons and should be approved and documented.

b. Immediately disabling or removing user IDs of users who have left the KCG.

c. Periodically identifying and removing or disabling redundant user IDs.

d. Ensuring that redundant user IDs are not issued to other users.

8.7.1.2 User Access Provisioning

The provisioning process for assigning or revoking access rights granted to user IDs shall include:

a. Obtaining authorization from the owner of the information system or service for the use of the information system or service.

b. Separate approval for access rights from management may also be appropriate.

c. Verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties.

d. Ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed.

e. Maintaining a central record of access rights granted to a user ID to access information systems and services.

f. Adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the KCG.

g. Periodically reviewing access rights with owners of the information systems or services.

8.7.1.3 Managed Privileged Access Rights

The KCG shall ensure the allocation of privileged access rights is controlled through a formal authorization process in accordance with the relevant access control policy. The following steps shall be considered:

a. The privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom they need to be allocated should be identified.

b. Privileged access rights shall be allocated to users on a need-to-use basis and on an event by event basis in line with the access control policy i.e. based on the minimum requirement for their functional roles.

c. An authorization process and a record of all privileges allocated should be maintained. Privileged access rights shall not be granted until the authorization process is complete.

d. Requirements for expiry of privileged access rights shall be defined;

e. Privileged access rights shall be assigned to a user ID different from those used for regular business activities. Regular business activities shall not be performed from privileged ID.

f. The competences of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties.

g. Specific procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to the systems configuration capabilities.

h. For generic administration user IDs, the confidentiality of secret authentication information shall be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

8.7.1.4 Management of Secret Authentication Information of Users

The KCG shall document a formal management process for the allocation of secret authentication information. It shall include the following:

a. Users shall be required to sign a statement to keep personal secret authentication information confidential and to keep group (i.e. shared) secret authentication information solely within the members of the group. This signed statement may be included in the terms and conditions of employment.

b. When users are required to maintain their own secret authentication information, they shall be provided initially with secure temporary secret authentication information, which they are forced to change on first use.

c. Procedures shall be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information.

d. Temporary secret authentication information should be given to users in a secure manner. The use of external parties or unprotected (clear text) electronic messages should be avoided.

e. Temporary secret authentication information should be unique to an individual and shall not be guessable.

f. Users shall acknowledge receipt of secret authentication information.

g. Default vendor secret authentication information shall be altered following installation of systems or software.

8.7.1.5 Review of User Access Rights

The KCG shall review user access rights at regular intervals. The review of access rights shall consider the following:

a. User access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment.

b. User access rights shall be reviewed and re-allocated when moving from one role to another within the KCG.

c. Authorizations for privileged access rights should be reviewed at more frequent intervals.

d. Privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained.

e. Changes to privileged accounts should be logged for periodic review.

8.7.1.6 Removal or Adjustment of Access Rights

The access rights of all employees and external parties to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

8.8 Physical and Environment Security

a. The KCG shall ensure that security perimeters or areas that contain either sensitive or critical information or information processing facilities are defined.

b. The date and time of entry and departure of visitors shall be recorded, and all visitors shall be supervised.

c. Access to areas where confidential information is processed or stored shall be restricted to authorized individuals.

d. All employees, contractors and external parties shall be required to wear some form of visible identification and shall immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.

e. External support service personnel shall be granted restricted access to secure areas or information processing facilities only when required. This access shall be authorized and monitored.

f. Access rights to secure areas shall be regularly reviewed and updated, and revoked when necessary.

g. The KCG shall establish measures to protect against external and environmental threats such as flooding, explosion, civil unrest and other forms of natural or man-made disaster.

h. Directories and internal telephone books identifying locations of information processing facilities shall not be readily accessible to anyone unauthorized.

i. The KCG shall establish procedures for secure removal of assets from information processing facilities.

j. The use of any mission critical information storing and processing equipment outside the KCG premises shall be authorized by management. This applies to equipment owned by the KCG and that equipment owned privately and used on behalf of the KCG.

k. Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturer's specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.

l. Logs shall be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

8.9 Cloud Security

The KCG shall ensure effective governance of cloud computing services, and that risk and compliance are catered for by taking the following measures into consideration:

a. Risk assessment of the cloud solution has been undertaken and the controls to the risks have been implemented.

b. Continued availability of the information systems and data by considering business continuity planning that seeks to prevent interruption of mission-critical services, and to re-establish full functionality.

c. Integrity of the information stored within the system and while on transit.

d. Confidentiality of sensitive data while stored and in transit.

e. Conformity to applicable laws and regulations.

f. If possible, include a right of audit in the contract.

g. Request proof of independent security reviews and certification reports that meet the KCG compliance requirement.

h. The use of private cloud deployment model only, no multi-tenancy, for additional security.

Abbreviations

BYOD	Bring Your Own Device
IaaS	Information as a Service
ICT	Information and Communication Technology
ICTA	Information and Telecommunication Authority
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISP	Internet Service Provider
KCG	Kisii County Government
LAN	Local Area Network
NAT	Network Address Translation
OEM	Original Equipment Manufacturer
OS	Operating System
PaaS	Platform as a Service
PC	Personal Computer
PII	Personally Identifiable Information
PCD	Personal Communication Device
PWD	Persons with Disabilities
QoS	Quality of Service
SaaS	Software as a Service
SLA	Service Level Agreement
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network