KISII COUNTY GOVERNMENT

DEPARTMENT OF FINANCE AND ECONOMIC PLANNING

DIRECTORATE OF INFORMATION COMMUNICATIONS TECHNOLOGY (ICT)

COUNTY ICT POLICIES AND PROCEDURES

OCTOBER 2017 – FINAL COPY

Tel: *0709 727 000 /11 or 0730 184 000 /11*
Email: *treasury@kisii.go.ke/ ict@kisii.go.ke*
Website: *www.kisii.go.ke*

Contents

LIST OF ACRONYMS AND ABBREVIATIONS

CD / CDROM	Compact Disk / Compact Disk Read Only Memory
COBIT	Control Objectives for Information and related Technology
DVD	Digital Video Disk
KCG	Kisii County Government
WAN	Wide Area Network
ICT	Information and Communication Technology
ISP	Internet Service Provider
IT	Information Technology
ITIL	IT Infrastructure Library
ITSM	IT Service Management
ISMS	Information Security Management System
ISO	International Standards Organization
LAN	Local Area Network
NGO	Non-Governmental Organization
PC	Personal Computer
SLA	Service Level Agreement
MDA	Ministry, Department or Agency
USB	Universal Service Bus
Val IT	IT Value Delivery

FOREWORD

The County Government of Kisii recognizes that the presence of a capable, effective, and forward-looking Public Service that will be able to implement the County Government's

development policies and deliver services in an efficient and timely manner, is a pre-requisite for fulfilling the good governance goals.
The Kisii County Government Integrated Development Plan have included provision of electronic services by the public service as one of the indicators for the growth of the ICT industry and overall economic growth of the county.
KCG ICT Standards focus on mainstreaming of ICT in the KCG to ensure that the county government realizes the potential of ICT in the efficient management of the public service and improvement of delivery of services to the general public.
The Policies and standards have been developed for specific critical areas of the KCG Public Service.
I would also like to thank Leading Consultants for their expertise in carrying out the development of the KCG ICT Policy and drafting the KCG ICT Standards.
Further appreciation goes to all KCG staff especially from the ICT department and their officers who participated in the development of these Policies and Standards.
It is my expectation that all Ministries, Departments and agencies will adhere to the Standards set here forthwith.

Signed

Robert Ombasa
Ag. COUNTY SECRETARY
KISII COUNTY GOVERNMENT

PREFACE

Kisii County Government has developed the KCG ICT Policies and Standards in order to ensure a systematic approach to ICT development, management and utilization in the KCG public service.
A consulting firm, Leading Associates and ICT department staff coordinated the development process. The process involved in-depth consultations conducted with stakeholders throughout Kisii County Government Public Service.
I trust that utilization of these Policies & standards will assist in improving the efficiency and effectiveness of ICTs as a crosscutting tool to the delivery of public service.

JOHN BILLY MOMANYI
CEC –FINANCE AND ECONOMIC PLANNING

1.0 INTRODUCTION

1.1 About Policies & Standards

A **Policy** is formal, brief, and high-level statement or plan that embraces governments' general beliefs, goals and objectives for a specified subject area. It focuses on desired results, not on means of implementation. Policies are further defined by standards and guidelines.

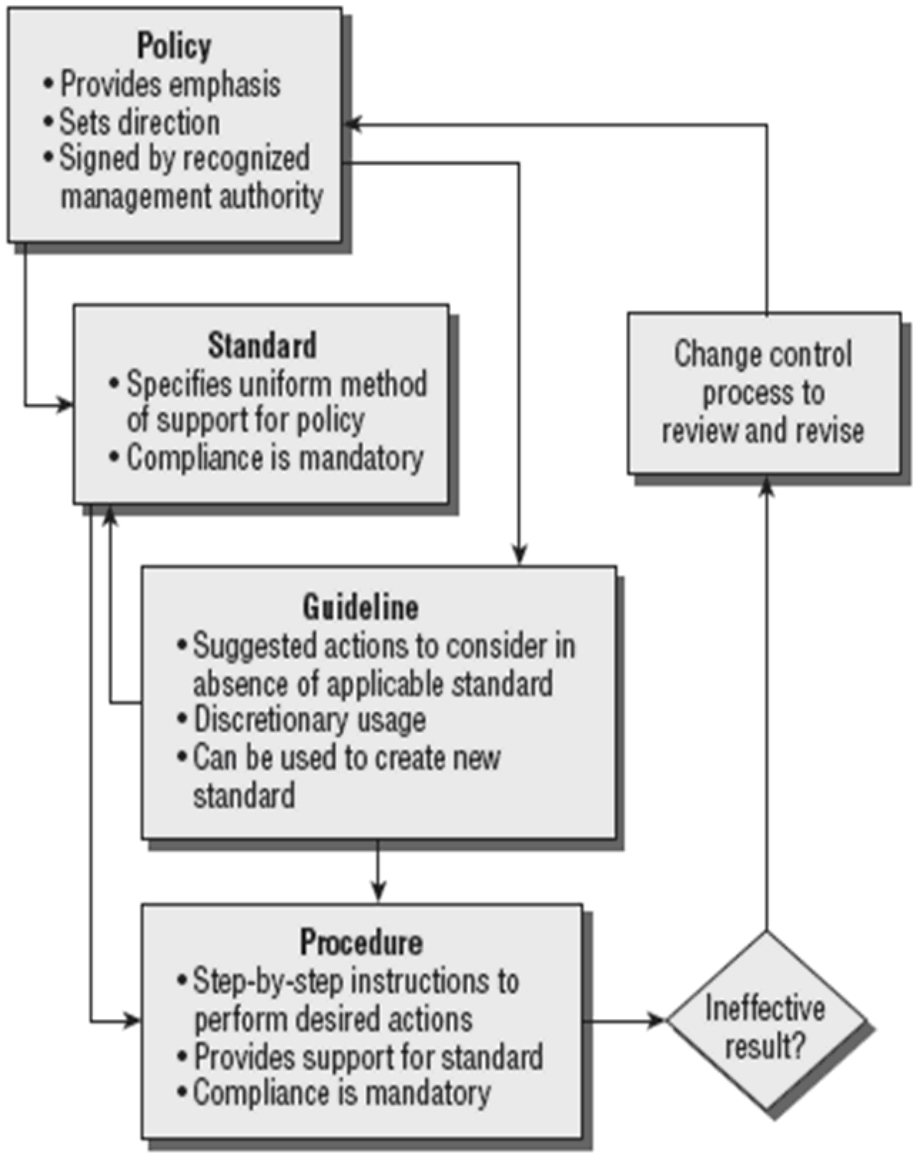


Figure 1: Linkages between policies, standards, guidelines and procedures

Standards define the process or rules to be used to support the strategic directions of government policies. A standard is meant to convey a mandatory action or rule and should be written in conjunction with a policy.

Guidelines provide general statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures.

Procedures are created from the standards and guidelines that support the policies. They are a series of steps taken to accomplish an end goal. Procedures define "how" to protect resources and are the mechanisms to enforce policy. They provide a quick reference in times of crisis.

1.2 Policy & Standards Domains

For purposes of covering all the necessary and important ICT related functions that required guidelines through a policy or standard, This document approached ICT functions as domains, namely; ICT budgets & inventory, critical ICT systems, ICT human resource & staffing and ICT security.

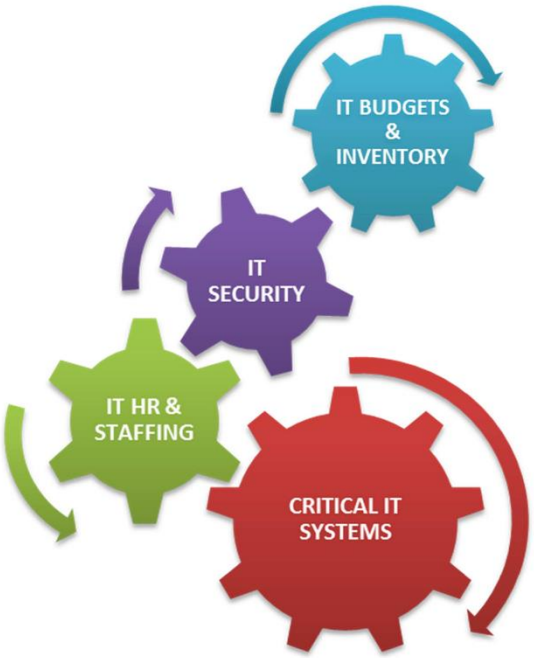


Figure 2: *ICT Policy & Standards Domains*

ICT Budgets & Inventory covers the process of equipment and system acquisition, replacement and disposal. Policies in this realm are concerned with budgeting, asset management, equipment replacement and disaster recovery and planning.

Critical ICT Systems refers to ICT operations that are deemed important for the operation of the County Government. These systems can be logically divided into Data, Process and Networks.

IT Security refers to both physical and network security of ICT assets that may contain data or be of value to the County government

ICT Human Resource refers to both the staff of the ICT department as well as users of equipment issued and maintained by the ICT department of the County.

2.0 SUMMARY OF THE POLICIES & STANDARDS

2.1 Acceptable use of ICT Facilities in the Public Service

This standard defines the control and protective measures for the use of ICT Equipment, Internet, E-mail, and other ICT resources to ensure that they are appropriately used for the purposes for which they were acquired. Information resources, all types of application software, hardware, network facilities, and similar devices, must be used appropriately, responsibly and with accountability.

2.2 Electronic Records Management

This Standard outlines the standards, including objectives, scope and structure, of the Document Management Process.
Furthermore, it identifies the various stages of a document life cycle that may apply to these documents and the standards and conventions that should be considered when creating or maintaining an electronic document intended for use or reference by more than one person within or outside the organization...

The security level of access to any document is to be determined prior to the publishing process. The intention is to provide a framework for the development and maintenance of electronic documents that are consistent and present a professional image appropriate to the intended audience.

The Standard is divided into three separate sections to enable the various ICT stakeholders to quickly go to the relevant section to find the information necessary to understand and comply with the requirements.

2.3 Information Asset Classification and Control

The Standard defines guidelines for the classification and management of sensitive information that is handled, created, received and/or destroyed by an organization in accordance with its sensitivity, confidentiality of content and business importance, based upon legislative, regulatory and contractual requirements.

2.4 Information System Security Management

The standard details the processes in place to ensure that ICT systems of an organization are maintained and operated in a secure manner.

2.5 Data Back-Up

The standard provides directions and guidance on the data back-up management (including restoration) performed by the ICT Staff working in an organization The standard does not include provision for hand-held devices.

2.6 ICT Audit

The Standard details the processes put in place to carry out ICT Audit. In line with rapid advancement of technology most organizations have become increasingly reliant on computerized information systems to deliver public services and carry out their daily operations. As a consequence, the reliability, integrity and availability of computerized data and of the systems that process, maintain and report these data are a major concern to audit. ICT Auditors examine the adequacy of controls in information systems and related operations to ensure system effectiveness.

ICT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively, and uses resources efficiently.

ICT auditing is a branch of general auditing concerned with governance (control) of information and communications technologies (computers).

2.7 ICT Project Management

The standard provides an overview of the essential components of the project management methodology used within an organization. The Standard includes the 'what', 'when' and 'why' of project management methodology. Examples of 'how' can be found in supporting procedures and forms. As a methodology, this Standard provides a structured approach to managing projects with ICT components.

2.8 System Development

The Standard defines what controls will be implemented by an organization in relation to System Development and Maintenance. This standard is consistent with, and should be read in conjunction with the Information Systems Security Standard. The Standard interprets current industry standards and recommends an application development standard for adoption in an organization for the software/application development lifecycle, consistent with the organization's enterprise architecture standards (in particular, compliance with the enterprise architecture checklist), principles, and best practices.

2.9 E-Waste Management

The Standard defines the obligations and processes to ensure that an organization disposes of unwanted and obsolete ICT electronic equipment and waste with due regard to environmental and security factors.

2.10 Strategic and Operational Planning

This Standard details the processes in place to ensure that ICT strategic and operational planning is aligned to an organization's business needs. The standard is intended to identify the various processes and activities performed within an organization that

influence the allocation of ICT resources towards ensuring projects and activities are aligned to achieving the business requirements of the organization..

3.0 THE POLICIES

3.1 Asset Management Policy

Document: Policy	Document No.: KCG IT-001	Revision: 1.00	Effective: [Signed Effective Date]

3.1.1 Administrative Use

This policy describes the asset management procedure to be used by the Kisii County Government.

3.1.2 Purpose

The asset management policy provides the overall framework for the management of IT equipment from procurement to disposal. This policy draws from the Financial Regulations and Information Security Policy. It defines roles and responsibilities that relate to the implementation of this policy.

a. Protecting county against loss of IT equipment assets;
b. Commitment to legal compliance;
c. Audit ability of asset use;
d. Management information.

3.1.3 Scope

This policy applies to, all staff and clients of Kisii county government who hold IT equipment purchased by the county

(a) All desktop and laptop PCs;
(b) All monitors, printers and scanners;
(c) All phones, mobile phones, smartphones;
(d) Any other IT peripheral.

This policy also applies to all IT equipment forming part of the county's IT infrastructure (Servers, network switches etc.) and equipment installed in IT classrooms and open access areas

Policies on asset management shall apply to the entire physical life cycle of all ICT assets distinct phases:

- Planning
- Acquisition
- Operation
- Disposal

3.1.4 Consequences

Misuse or abuse of County Government IT assets through willful violation of the asset Policy will result in disciplinary action leading up to and/or including termination, the

surrender of applicable evidence for County or federal criminal investigations, or further legal action.

3.1.5 Objectives

- Improve ICT security through advanced ICT Asset control
- Improve financial planning through clear identification of all assets and their associated relationships
- Improve software license management ensuring legal compliance.
- Increase confidence in ICT Systems and ICT Services
- Increase customer satisfaction

3.1.6 Responsibility and Authority

It is the responsibility of the _____(*executive authority*) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted.
It is the responsibility of the ICT DIRECTOR (Technical authority) to verify the practices and procedures to execute this Policy

3.1.7 Policy Statements

a. All ICT hardware items are to be procured via the ICT department.
b. Any request for new equipment needs to be given to the ICT department, ICT will forward the specifications and other details to procurement for purchase
c. Departments other than ICT are specifically prohibited from purchasing any of the following equipment. PCs, monitors, printers, scanners and all associated cabling Laptop computers phones and digital cameras.
d. Hardware asset tags will be affixed to PCs and laptops on receipt. These tags will identify the asset with a unique asset number. A continually-running inventory system will be used to maintain a register of PCs and laptops, and the software installed on them. This audit information will be checked at least twice yearly against the License Dashboard to ensure that there is a match between software installed and software licenses owned.
e. Accurate, Updated and maintained inventory should be kept for all ICT equipment
f. All ICT equipment shall be signed for (without amendment) by equipment holders and declaration is scanned into the inventory management system;
g. Reports on any assets stripped for spares should be documented and components removed noted within the asset management system. Data on harvested drives will immediately have data destructed using a method approved by the PICTO hardware and user support;
h. All unwanted / redundant ICT related assets are to be disposed of by the ICT department, in accordance with the appropriate procedure.
i. After purchase on collection all new equipment should be signed for by IT staff. IT equipment will not be issued by the purchasing team to porters or end users.
j. Before any Issuance all equipment should be tagged and referenced in the system.
k. Any Loss or theft of IT equipment must be reported immediately to the PICTO Hardware and support

l. All ICT equipment (including portable devices) must be returned to the relevant IT support team upon replacement, equipment redundancy or when the holder loses affiliation to the county.
m. Equipment holders will retain responsibility for equipment issued to them until it has been returned to ICT department for redeployment or disposal
n. It is the responsibility of the County ICT technical authority and the respective line manager with the appropriate authority to ensure that IT assets, equipment, and hardware are replaced of according to one or more of the procedures prescribed below. It is imperative that any replacement performed by the Kisii County Government be done appropriately, responsibly, and ethically, as well as with County Government resource planning in mind. The following rules must therefore be observed:

1. *Obsolete IT Assets:*

As prescribed above, "obsolete" refers to any and all computer or computer-related equipment over [3] years old and/or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as obsolete is the sole province of the County Governments IT department. Decisions on this matter will be made according to the County Government's purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.

2. *Reassignment of Retired Assets:*

Reassignment of computer hardware to a less-critical role is made at the sole discretion of the County Government's IT department. It is, however, the goal of the County Government to – whenever possible – reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will do instead.

3. *Trade-Ins:*

Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement. The County Government's purchasing and Procurement manager or IT Asset manager will assume this responsibility.

4. *Cannibalization and Assets beyond Reasonable Repair:*

The IT manager is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as such should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the organization. The IT department will inventory and stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means will be subject to the Counties disposal procedure.

3.1.8 Standards for Asset Management Disposal

1. Rationale

Standardize disposal, and ensure compliance with relevant Statutes

2. Brief description of standard

Disposal and de-commissioning of ICT products and services

Disposal of all government IT assets should be guided by Public Procurement & Disposal Act and Regulations and MDA's disposal procedures.

3.1.9 Asset Management

1. Rationale

All assets should be accounted for, have a nominated owner and used in an acceptable manner.

2. Brief description of standard

MDAs will have a process to ensure maintenance and protection of all ICT assets under their jurisdiction.

The standard gives guidelines on the proper management ICT assets under the MDA's jurisdiction.

3.10 Procurement (L/P/001)

1. Rationale

Standardize procurement and ensure compliance with statute

2. Brief description of standard

Procurement of ICT goods and Services

All procurement procedures for ICT assets should be guided by Public Procurement & Disposal Act and Regulations.

3.11 ICT Asset Disposal Procedure

a. The PICTO in charge of Hardware and support reports of unserviceable or obsolete equipment to the attention of the disposal committee.
b. The disposal committee shall recommend to the accounting officer a method of disposing of the stores and equipment which may include any of the following
    - transfer to another public entity or part of a public entity, with or without financial adjustment;
    - sale by public tender;
    - sale by public auction; or
    - destruction, dumping or burying;
    - Trade-in.

c. Within the prescribed time period after receiving the recommendations of the disposal committee the accounting officer shall give the committee a written notice as to whether the accounting officer accepts or rejects the recommendations of the committee.
d. If the accounting officer accepts the recommendations of the disposal committee, the equipment shall be disposed of in accordance with those recommendations.
e. the disposed item should be indicated in the inventory management that it has been disposed
f. If the accounting officer rejects the recommendations of the disposal committee he shall,
g. include, with the notice given to the committee, written reasons for rejecting the recommendations of the committee;
h. give the authority a copy of the notice under and the written reasons
i. Refer the matter back to the committee for further consideration.

3.2 Backup Policy

Document: Policy	Document No.: KCG IT-002	Revision: 1.00	Effective: [Signed Effective Date]

3.2.1 Introduction

Computer information systems and electronic data are valuable assets to the Kisii county Government and a substantial investment in the county's human and financial resources that has been made to create these systems and information and, as such, a formalized policy has been implemented to:

- Safeguard the risk of losing data.
- Safeguard the confidentiality and integrity of information contained within these systems.
- Ensure availability of critical data so that information can be utilized as the valuable asset that it is will reduce business and legal risk.
- Departmental critical data and non-departmental critical data are stored on Fileservers, Exchange-servers (mail-box data) and Application-servers. This data can be categorized as: *Personal User data, Business Unit data, Shared data, Databases, Application / System data*.

3.2.2 Scope

The goal for the ICT Department is:

- To offer user support and to ensure that departmental data can be recovered within required and agreed business timescales.
- Responsible for backing up File-servers, Exchange-servers and Application-servers, according to agreed cycles, and storing these backups in a secure designated area.
- Perform regular disk capacity management on all data servers and have the right to delete all non-departmental related data after consultation with involved employees. If the disposal of old or damaged tapes is

required, such tapes will be destroyed to prevent the recovery of data from the media.

Ownership of all electronic information residing on any departmental/ministerial computer system vests in Kisii county Government and Management may peruse, monitor and take copies of any information or communication made or received utilizing any of the aforementioned systems. Therefore, ICT department requires

A backup policy that all requests to restore an employee's user data, residing on File-servers or Exchange-servers (mail-box data), not requested by the employee or without the permission of such employee, must be authorized by the ICT Director.

This policy defines the backup strategy for servers and data within Kisii County Government.

3.2.3 Definitions

Backup – is the process of copying active files from online disk to tape so that files may be restored to a disk in the event of equipment failure, damage to or loss of data.

Archive – is the process of moving inactive files form online disk to a tape, i.e. deleting the files from copying them, in order to release online storage for reuse.

Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

3.2.4 Timings

A *grandfather -father-son* rotation scheme is operated; incremental backups run overnight from Monday to Thursday (daily backup) and full back up (i.e. weekly backup) run on Fridays are rotated on three weeks basis. One full back up each month (i.e. Monthly backup) will be made.

3.2.5 Data Backed up

Data to be backed up include the following:

- Users data stored on the home directories ("My Documents")
- System state of all servers

Systems to be backed up include:

- Mail Exchange Server
- Mailboxes
- Network File Server
- Application Server
- Proxy Server
- Firewall

3.2.6 Excluded extensions

On home directories folders ("My Documents") not all files will be backed up; the following are extensions that will be omitted:

Mpeg, Mpa, Mp2, Mp3, Mp4, Exe, Vob, Wsf, Wma, Wav,

3.2.7 Procedures

Incremental backups will be performed daily from Monday to Thursday. The network drive will be add-on with new information created.
A full systems and data backup will be performed weekly. Weekly backups will run on Fridays and the disks will be monitored for space availability.
Monthly backups will be made on the last Friday of each month and stored for a minimum period of 5 (five) years thereafter it will be handed to the archives and archived where required under the classification system as in use by the Kisii County Government Administration.

Refer to table in screen shot.

3.2.8 Network Drive Storage

All weekly and monthly back-ups will be stored in the File Server in the data center which will be fire proof and safe at Kisii County Government ICT Department.

3.2.9 Responsibility

The PICTO Systems Admin shall delegate an ICTO to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis. The designated person will take weekly and monthly tapes to offsite storage.

The staff of the specific department who has any business critical data on local computer and notebook hard drives must be copied or moved to a "My Documents" share on a file server, where it will be backed up. Where such an action is not possible, as in cases where it is done away from access to Kisii County Government network, the data must be copied over on the first available opportunity. It will be the sole responsibility of the county staff, under all circumstances, to backup and maintain security regarding personal data. In addition to workstations, county staff have been allocated space per user, secured per user logon ID, on the File-servers. The onus is on the employee to ensure that the server space allocated is utilized to the optimum.

3.2.10 Restorations

Users that need files restored must submit a request to the IT help desk by completing a Data Restore Request Form. Information regarding the request where possible must include the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

3.3 Cloud Computing Services Policy

Document:	Document No.:	Revision:	Effective:
Policy	KCG IT-003	1.00	[Signed Effective Date]

3.3.1 Purpose

The purpose of this policy is to guide KCG ICT staff in the appropriate manner of storing data or information in non-KCG storage facilities, often referred to as 'the cloud', 'cloud computing' or outsourcing.

This policy also provides a checklist of recommendations when considering engaging in use of such services; however it is strongly recommended that ICT staff seek expert advice when using these services.

3.3.2 Organizational Scope

This policy applies to all KCG data or information resources which are stored with or hosted by any party other than KCG within one of its Data Centres.

3.3.2.1 Definitions

- Cloud - A style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to customers using Internet technologies. The Internet has always been diagrammatically described as a cloud, hence the term that a service can be hosted 'somewhere in the cloud', or externally hosted
- Outsourced - The service is delivered by an external IT organization using either the vendors' infrastructure or KCG infrastructure.
- In-sourced Service - The service is delivered by KCG using KCG infrastructure
- Private Cloud - The underlying infrastructure is dedicated to a single customer/entity.
- On Demand - Able to request increased infrastructure and services as demand grows whilst such cloud services are attractive, for a range of reasons, thorough investigation is required by the services of a provider are engaged (free or costed) as there are many legislative and reputation issues in the failure of such a service.
- Community Cloud - The underlying infrastructure is shared by the county e.g. Huduma Center. Where there is a need to actually share information or services across the county. This will become more important with the increased need for sharing of government data, in particular
- Public Cloud - The infrastructure is shared by a service providers' customer base in general

3.3.3 Scope

This policy does not intend to be prescriptive in describing the process for the engagement of a provider of a cloud service, but to point KCG toward qualified staff to advise the appropriate strategy to utilize a cloud based service.

3.3.4 Content

KCG provides facilities for secure storage of data and information, however it is recognised that there may be instances where staff need to use applications which store data in non-KCG-owned facilities. These services include, but are not limited to:

a. Consumer services such as: Google Docs, Dropbox, Gmail, Hotmail, iCloud, MobileMe, etc.
b. The New Zealand Government Cloud Programme which offers storage or services on a pay-per-use or subscription basis.
c. Software as a Service (SaaS) applications which store data in non-KCG-Owned facilities such as Project Management software, Customer Management Software, Patient Management software, Task Software or Reader Software etc.

Use of outsourced data storage or cloud computing resources must be in compliance with all other KCG policies and procedures and relevant legislation. It is the responsibility of KCG staff using such services to ensure that they are aware of, and are fully compliant with all relevant policies, procedures and legislation.

Staff who use cloud computing or outsourcing facilities are also responsible for ensuring compliance with the following:

3.3.4.1 Evaluation Process:

a. When deciding to use a cloud-based service or to store information or data in a facility which is not owned by KCG, it is the responsibility of the staff member using the service or storing the information or data to consult with appropriate ICTOs', process owners, stakeholders, and subject matter experts during the evaluation process.
b. The Registrar or the Director of Information Technology Service should also be consulted for guidance.
c. The consultation and decision to store data in a non-KCG facility must be documented.

3.3.4.2 Intellectual Property and Copyright:

a. Information or data must not be stored in any facility where KCG's intellectual property, copyright, trademarks or patents may be compromised.
b. Information or data may not be stored in such a way that allows unauthorised parties to claim ownership of the information or data.
c. When information or data is stored in a facility which is not owned by KCG, it is the responsibility of the staff member storing the information or data to ensure that no contract or legal agreement is entered into which may compromise KCG's intellectual property, copyright, trademarks or patents.

3.3.4.3 Privacy and Data Security:

a. Information or data that has been marked as confidential, sensitive or secret may not be stored in such a way that the information or data could be accessed by any unauthorised parties.
b. KCG information, staff information, or any other personally identifying information must be stored in a manner which fully protects the privacy of the individual and is fully compliant with all relevant privacy legislation.
c. It is the responsibility of the staff member storing the data to ensure that physical and logical security measures adequately protect the information being stored. Staff should consult with Information and Communication Technology Services where any security issues are unclear.
d. Staff should consult with the Registrar for assistance where Privacy issues are unclear.

3.3.4.4 Records Retention and Availability:

a. All Public Records whether instructional, administrative, or research must be stored and retained according to KCG's Records Management Policy and the General Disposal Authority.

3.3.5 Requirements of Cloud Services:

The following guidelines are intended to assist units in their approach to evaluating the prudence and feasibility of using cloud computing services. This is not an exhaustive list and it is recommended that staff consult with the Director of Information and Communication Technology when considering the use of cloud-based services.

a. Cloud based services may have 'click-to-accept' agreements that incur legal obligation or risk. By accepting such terms, staff could be held personally liable.
b. Ensure a Service Level Agreement (SLA) with the vendor exists that requires:
   (i) clear definition of services
   (ii) agreed upon service levels
   (iii) clearly defined physical and logical security conditions
   (iv) performance measurement
   (v) problem management
   (vi) customer duties
   (vii) disaster recovery
   (viii) termination of agreement
   (ix) protection of sensitive information and intellectual property
   (x) agreement of the disposal of information when required
   (xi) Definition of vendor versus customer responsibilities, especially pertaining to backups, incident response, and data recovery.

c. An exit strategy for disengaging from the vendor and/or service should be planned before committing information or data to a cloud computing or outsourced service. The exit strategy should outline how the relevant records will be preserved and maintained, and how the service can be discontinued or transitioned to another provider.

3.4 Data Center Access Policies and Procedures

Document:	Document No.:	Revision:	Effective:
Policy	KCG IT-004	1.00	[Signed Effective Date]

3.4.1 Overview

The procedures described in this document have been developed to maintain a secure Data Center environment and must be followed by individuals working in the Data Center. It is important that any department/project envisioning the installation of their servers in the Data Center fully understand and agree to these set procedures.

3.4.2 Data Center Physical Security Policy and Procedure

Security for the Data Center is the Responsibility of the Data Center Management Team. The Head of ICT is responsible for the administration for this policy. The following are the general requirements, policies and practices that govern access to this sensitive area, for which the ICT Department has responsibility. It is important that all departments, staff and business associates follow these policies and practices.

3.4.3 Primary Guidelines

The "Data Center" is a restricted area that requires a much greater level of control than normal non-public premises. Only those individual who are expressly authorized to do so may enter this area. Access privileges will be grated to individuals who have a legitimate business need to be in the data center. Furthermore, this area may only be entered to conduct authorized Foundation business. Any questions regarding policies and procedures should be addressed with the ICT Head. The only exception allowed to the Data Center Security Policies and Practices is temporary suspension of these rules if it becomes necessary to provide emergency access to medical, fire and/or police officials, etc.

3.4.4 Levels of Access to the Data Center

There are 3 "Levels of Access" to the Data Center in Kisii County Government – General Access, Limited access, and Escorted Access

3.4.4.1 General Access is given to people who have free access authority into the Data Center. General Access is granted to the ICT Staff whose job responsibilities require that they have access to the area. Individuals with Limited access will be granted a different key combination for the data center door. Individuals with General access to the area may allow properly authorized individuals escorted access to the data center. If a person with General Access allows Escorted access to an individual the person granting access is responsible for escorting the individual granted access and seeing to it that the protocol is followed.

3.4.4.2 Escorted Access is closely monitored access given to people who have a legitimate business need for infrequent access to the Data Center. "Infrequent access" is generally defined as access required for less than 15 days per year. Individuals with Escorted Access will not be issued a door combination to access the data center with. A person given Escorted Access to the area must sign in and out under the direct supervision of a person with General Access, must provide positive identification upon demand, and must leave the area when requested to do so. Individuals allowed Escorted Access will be placed on the ITS Operations.

3.4.4.3 Limited Access is granted to a person who does not qualify for General Access but has a legitimate business reason for unsupervised access to the Data Center. Unescorted Access personnel cannot authorize others to be granted unsupervised access to the Data Center. Unescorted access personnel can only grant escorted access to individuals where related to the grantor's business in the Data Center.
The grantor is responsible for these individuals and must escort them in the Data Center at all times Students who are given Limited Access may NOT escort anyone into the Data Center without approval.

3.4.5 Data Center Door

All doors to the Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:
Allow officially approved and logged entrance and exit of authorized individuals
Permit the transfer of supplies/equipment as directly supervised by a person with General Access to the area

Prop open a door to the Data Center ONLY if it is necessary to increase airflow into the Data Center in the case on an air conditioning failure. In this case, staff personnel with General Access must be present and limit access to the Data Center.

3.4.6 Exception Reporting

All infractions of the Data Center Physical Security Policies and Procedures shall be reported to the Data Center Management Team. If warranted (e.g.: emergency, imminent danger, etc.) the county police should be notified as soon as is reasonably possible.
When an unauthorized individual is found in the Data Center it must be reported immediately to a member of the Data Centre Management Team. If this occurs during the evening hours, a Senior Operator or the Operations Manager should be contacted. They will determine if the police should be contacted. The unauthorized individual should be escorted from the Data Center and a full written report should be immediately submitted to the Data Center Management Team. Individuals with General Access to the area are to monitor the area and remove any individual who appears to be compromising either the security of the area or its activities, or who is disrupting operation. It is particularly important that individuals with General Access show initiative in monitoring and maintaining the security of the Data Center.

3.4.7 Requesting Access to the Data Center

Departments/projects that have computer equipment in the Data Center may request access to the Data Center. The individuals designated by the requesting department/project will be granted access once the ICT Data Center Management authorizes them.
Upon approval by the Data Center Management, an appointment with the person requesting access will be effected in order to provide the person with a copy of the Kisii County Government Data Center Access Policies.
When a person who has access to the Data Center terminates his employment or transfers out of the department, the person's department must notify the Data Center Management Team as soon as possible so that the person's access to the Data Center can be removed. This is extremely important in cases where the employee was terminated for cause.

3.4.8 General Data Center Operations Policies for Departments/Projects

General Hosting Policy for Data Center Capacity Planning ITS Operations must be consulted for any new equipment to be installed in the Data Center. It is advisable to consult with ITS Operations as early as possible (preferably months before actual equipment is ordered), to confirm your equipment actually can be hosted.

3.4.9 General Policy on Infrastructure Work

In The Data Center ITS Operations must be notified of all work pertaining to infrastructure in the Data Center. This includes things such as equipment installation/removal, construction or any activity that adds/removes assets to/from the Data Center.

3.4.10 General Safety Policy

All individuals in the Data Center must conduct their work in observance with all applicable policies related to safety.

3.4.11 General Cleanliness Policy

The Data Center must be kept as clean as possible. All individuals in the Data Center are expected to always keep clean the vicinity. Boxes and trash need to be disposed of properly. Tools must be replaced to their rightful place. Food and drink are not allowed in the Data Center.

3.4.12 Policies for Data Center Equipment Deliveries/Pick-Up

Any department that is planning to have equipment delivered to or picked up from the Data Center should contact ITS Operations and provide details to ITS Operations in advance of delivery/pick-up. Please provide ITS Operations with the following information for the equipment log: For the delivery of equipment:

Expected day of delivery
P.O. number for the equipment (if known)
Vendor name and description of the equipment
Person to be contacted when the equipment arrives

For the pick-up of equipment:

Expected day the equipment will be picked up
Vendor name and the description and location of the equipment to be picked up.
Name of person to be notified once equipment is picked up

3.5 Disaster Recovery and Business Continuity Policy

Document:	Document No.:	Revision:	Effective:
Policy	KCG IT-005	1.00	[Signed Effective Date]

3.5.1 Administrative Use

This policy describes the disaster recovery procedure to be used by the Kisii County Government. It should be acknowledged and executed by a section head.

3.5.2 Normative References

Proposed Abridged ICT Standards for GoK

1. **Backup and Restoration DM/BAR/001** - This standard outlines specifications for data backups and restoration aligned with business requirements
2. **Business Continuity & Resilience (IO/BC/001)**
3. **Disaster Recovery Period (IO/DR/002)**

3.5.3 Purpose

To minimize the impact of significant incidents on County Government services and recover from unavailability of IT systems to an acceptable level through a combination of responsive and recovery controls

3.5.4 Scope

This Policy applies to all of the data/services deemed mission-critical by the County Government at all of its locations. This Policy only applies to centralized data

maintained on County Government servers and SAN/NAS, and that is under the jurisdiction and knowledge of a section head.

3.5.5 Consequences

Any contravention of this policy will be dealt with under the appropriate procedures. This may involve the disciplinary procedure being invoked which may range from informal warning to summary dismissal.

3.5.6 Objective

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the County government recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

a. The need to ensure that all employees fully understand their duties in implementing such a plan
b. The need to ensure that operational policies are adhered to within all planned activities
c. The need to ensure that proposed contingency arrangements are cost-effective
d. The need to consider implications on other company sites
e. Disaster recovery capabilities as applicable to key customers, vendors and others

3.5.7 Definitions

3.5.7.1 Disaster

A disaster refers to an event which leads to an extended loss of service or loss of critical data and cannot be managed within the scope of normal working operations.

3.5.7.2 Mission-Critical Data

The following forms of information are deemed operationally critical by the County Government management and are therefore subject to this Policy:

[*Note: This section attempts to classify the applications, databases, and data structures in use in your facility. Identify them here. Technical Manager to specify more detail*]

Critical IT System	Grade
IPPD HR System	A
GPay	A
CIFMIS	A
Shared File System	B
Network Operating System (NOS) Directories, Keys, and Lists	C
Active Directory	C
...[more]	...[more]

3.5.8 Responsibility and Authority

It is the responsibility of the _____(*executive authority*) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted. It is the responsibility of the ICT DIRECTOR (Technical Authority) to verify the practices and procedures necessary to execute this policy.

3.5.9 Policy Statements

a. The Kisii County Government shall develop a comprehensive IT disaster recovery plan
b. A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan
c. The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks
d. The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
e. All staff must be made aware of the disaster recovery plan and their own respective roles.
f. The disaster recovery plan is to be kept up to date to take into account changing circumstances.

3.5.10 Disaster Declaration

The following employees of Kisii County Government are authorized to declare an Information Technology Systems Disaster and also signal a resumption of normal processing:

NO	NAME	POSITION

3.5.11 Plan Activation

Disaster Recovery plan will be activated in response to internal or external threats to the Information Technology Systems of Kisii County Government. Internal threats could include fire, bomb threat, and loss of power or other utility or other incidents that threaten the staff and/or the facility.
External threats include events that put the facility in danger. Examples might include severe weather or a disruptive incident in the community.
Once a threat has been confirmed, the disaster recovery plan management team will assess the situation and initiate the plan if necessary.

3.5.12 Resumption of Normal Operations

Once the threat has passed, equipment has been repaired or replaced or a new data center has been built and stocked, the disaster recovery team will assess the situation, declare the disaster over and resume normal operations.

3.5.13 Disaster Recovery Strategy

The overall disaster recovery strategy of Kisii County government is as below;

3.5.13.1 Data Center Disruption

- Failover to alternate Data Center
- Reroute core processes to another Data Center (without full failover)
- Operate at a deprecated service level
- Take no action

3.5.13.2 Significant Dependency (Internal or External) Disruption

- Reroute core functions to backup / alternate provider
- Participate in recovery strategies as available
- Wait for the restoration of service, provide communication as needed to stakeholders

3.5.13.3 Significant network or other issues

- Reroute operations to backup processing unit / service (load balancing, caching)
- Wait for service to be restored, communicate with core stakeholders as needed

3.5.14 Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan.

3.5.14.1 Response Phase: The immediate actions following a significant event.

- On call personnel paged
- Decision made around recovery strategies to be taken
- Full recovery team identified

3.5.14.2 Resumption Phase: Activities necessary to resume services after team has been notified.

- Recovery procedures implemented
- Coordination with other departments executed as needed

3.5.14.3 Restoration Phase: Tasks taken to restore service to previous levels.

- Rollback procedures implemented
- Operations restored

3.5.15 Disaster Recovery Operations

a. All activities and steps necessary to restore systems services that are affected by a disaster.
b. All activities concerned with management and user communications related to the disaster.
c. All activities concerned with the mitigation of the impact of an ongoing disaster incident.
d. All activities concerned with the follow-up to an incident.

3.5.16 Procedures in the implementation of a disaster recovery policy

a. Setup and maintain offsite facilities for data backup storage and electronic vaulting as well as redundant and reliable standby systems if necessary.
b. Ensure that critical applications, systems, and data are distributed among facilities that are reasonably easy to get to but not so close that they could be affected by the same disaster.
c. Establish written policies, contracts, and service level agreements with third party hosting, collocation, telecommunications, and Internet service providers that facilitate prompt recovery and continuity.
d. Create an incident response team that consists of information security, IT, marketing, HR, legal, and other relevant personnel.
e. Define the roles and responsibilities of the incident response team.
f. Obtain each incident response team member's contact information.
g. Determine which methods the incident response team members will use to communicate in the event of a disaster.
h. Create a public relations plan to assist with the effective handling of an incident.
i. Assign a manager (such as an IT Manager) that has the responsibility and authority to make critical IT decisions.
j. Develop testing standards.
k. Document and distribute the disaster recovery plan.
l. Distribute copies of the written plans to everyone involved and also store extra copies in an offsite, fireproof vault.

3.5.16.1 The following are ongoing procedures that must be followed:

a. Continuously perform data backups, store at least weekly backup's offsite, and test those backups regularly for data integrity and reliability.
b. Test plans at least annually, document and review the results, and update the plans as needed.
c. Analyze plans on an ongoing basis to ensure alignment with current business objectives and requirements.
d. Provide security awareness and disaster recovery education for all team members involved.
e. Continuously update information security policies and network diagrams.
f. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
g. Perform continuous computer vulnerability assessments and audits.

3.5.17 Disaster Recovery Standards

3.5.17.1 Disaster Recovery Plan – Policy Standards

a. Each department shall have a documented disaster recovery plan.
b. Each department's disaster recovery plan shall include a clear definition for disaster, specific to your facilities and technology configuration.
c. Each department's disaster recovery plan shall be accessible in the event of a disaster.
d. Each department's appropriate staff shall be trained on the disaster recovery plan.

e. Each department's disaster recovery plan shall include responsibilities, authorities, and accountabilities during contingency operations.

f. Each department shall have vendor maintenance contracts to address equipment and/or system failures.

g. Each department's disaster recovery plan shall address the need for an alternative recovery site.

3.5.17.2 Disaster Recovery Plan - Procedural Standards

a. Each department's disaster recovery plan shall include the technology needed for off-site storage.

b. Each department's disaster recovery plan shall include a physical layout (e.g. blue print) of the offsite storage facility.

c. Each department's disaster recovery plan shall include a logical layout (e.g. connectivity and wiring diagram) of the offsite storage facility.

d. Each department's disaster recovery plan shall include media rotation procedures for off-site storage.

e. Each department's disaster recovery plan shall specify retention periods for all critical records.

f. Each department's disaster recovery shall plan include provisions for adequate inventory of critical business forms.

g. Each department's disaster recovery plan shall include requirements to maintain up-to-date hard copies of all business critical documents-including application program source code.

h. Each department's disaster recovery plan shall include requirements to maintain copies of critical reference material in an off-site location.

i. Each department's disaster recovery plan shall include requirements to maintain contact information-personnel, hardware/software, venders, utilities, etc.

j. Each department's disaster recovery plan shall include requirements to maintain copies of critical business procedures.

k. Each department's disaster recovery plan shall include procedures to process paper transactions (e.g. manual procedures) of critical business functions.

l. Each department's disaster recovery plan's "alternate work procedures" shall include a prioritized list of business interfaces.

m. Each department's disaster recovery plan "work around procedures" shall include a list of equipment required to process business critical functions.

n. Each department's disaster recovery plan's "work around procedures" shall include a list of business critical forms.

o. Each department's disaster recovery plan's "work around procedures" shall include a list of personnel and alternate personnel required to support business critical functions.

p. Each department's disaster recovery plan's "work around procedures" shall include a list of services required to support business critical processes- phone, electricity, mail, etc.

q. Each department's disaster recovery plan "work around procedures" shall include a list of communications required to support business critical functions.

r. Each department's disaster recovery plan shall include an emergency notification process, personnel and staffing response, meeting locations, and assigned responsibilities.

s. Each department's disaster recovery plan's "work around procedures" shall include hardcopy and local backup strategies for business critical functions.

t. Each department's disaster recovery plan shall include key vendor information (e.g. name, phone numbers, product, and serial numbers) to support business critical functions.

u. Each department's disaster recovery plan shall identify the necessary resources required to support the recovery mode.

v. Each department's disaster recovery plan shall include provisions for all human elements required to support the business critical functions - who, what, where, and contact information.

w. Each department's disaster recovery plan shall include business function support team composition (functional and technical members) including skill set match, training, and testing capabilities.

x. Each department's disaster recovery plan shall include procedures and policies regarding the authorization to initiate contingency operations and resume normal operations.

y. Each department's disaster recovery plan shall include quantifiable service level thresholds for contingency operations activation/deactivation.

z. Each department's disaster recovery plan shall include specific triggers to activate/deactivate the contingency operations.

aa. Each department's disaster recovery plan shall include methods for quantifying degradation of service.

bb. Each department's disaster recovery plan shall include responsibilities, authorities, and accountabilities during contingency operations.

cc. Each department's disaster recovery plan shall include methods, policies, and procedures for voice communication to support critical business functions especially as they pertain to business continuity plans.

dd. Each department's disaster recovery plan shall include business continuity plan distribution policies and procedures.

ee. Each department's disaster recovery plan shall include business continuity plan maintenance policies and procedures.

ff. Each department's disaster recovery plan shall include business continuity plan testing policies and procedures.

gg. Each department's disaster recovery plan shall include business continuity responsibility policies.

hh. Each department's disaster recovery plan shall include documented facility security procedure.

ii. Each department's disaster recovery plan shall include documented security policies and procedures for the transfer of media to an alternate facility.

jj. Each department's disaster recovery plan shall have a distribution procedure for the plan.

kk. Each department's disaster recovery plan shall have a process for maintaining and updating the disaster recovery plan.

ll. Each department shall periodically test the disaster recovery plan.

mm. Each department shall document roles and responsibilities for the execution of the disaster recovery plan.

nn. Each department's disaster recovery plan shall document appropriate decision making authorities.

oo. Each department's disaster recovery plan shall document hardware restoration and replacement procedures including service requests, purchase orders, and supply chain.

pp. Each department's disaster recovery plan shall include documented procedures for returning from the alternate site.

qq. Each department's disaster recovery plan shall include documented procedures for parallel processing when returning from an alternate site.

rr. Each department's disaster recovery plan shall include documented procedures for cut over processing when returning from an alternate site.

ss. Each department's disaster recovery plan shall include documented procedures for an alternative site shutdown.

tt. The disaster recovery plan shall include documented procedures for data disposition including delete/scratch controls and physical handling to/from an alternate site.

uu. Each department's disaster recovery plan shall include documented hardware backup strategies.

vv. Each department's disaster recovery plan shall include documented software backup strategies.

ww. Each department's disaster recovery plan shall include documented network backup strategies.

xx. Each department's disaster recovery plan shall include documented testing procedures.

yy. Each department's disaster recovery plan shall include documented maintenance procedures.

zz. Each department's recovery strategy shall be mapped to the appropriate risk.

aaa. Each department's disaster recovery plan shall include asset management inventory procedures.

bbb. Each department's disaster recovery plan shall include procedures for returning to normal operations.

ccc. A plan for managing identified risks shall be developed.

ddd. The critical business application's downtime procedures shall be determined and documented.

eee. The time threshold for invoking business critical application downtime procedures shall be determined and documented.

fff. Detailed action plans shall be documented to get the school/department/center to define minimum acceptable levels of service.

ggg. Minimum acceptable levels of system availability shall be defined.

3.6 Email Policy Document

Document: Policy	Document No.: KCG IT-006	Revision: 1.00	Effective: [Signed Effective Date]

3.6.1 Administrative Use

This policy describes the Email procedure to be used by the County Government as a means of communication both internally and externally. It should be acknowledged and executed by a County section head.

3.6.2 Purpose

The purpose of this policy is to ensure the proper use of County Government email system and make users aware of what County Government deems as acceptable and unacceptable use of its email system.

3.6.3 Scope

This Policy covers the use of all email addresses issued by the County Government to all of its individual and locations. This Policy only applies to County Government email and no other email service providers accessed through county devices, and that is under the jurisdiction and knowledge of a section head.

3.6.4 Consequences

An employee found to have violated this policy may be subject to disciplinary action leading up to termination of employment

3.6.5 Objective

The broad goals of this policy are:

- Improve the successful delivery of Kisii County Government communications to all departments, sub-counties, staff and any other agents operating on behalf of the Kisii County Government
- Reduce the risk of data classified as legally restricted or confidential going through email systems that are managed by the County government.

3.6.6 Responsibility and Authority

It is the responsibility of the department heads (*executive authority*) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted. It is the responsibility of the Systems Administrator to verify the practices and procedures necessary to execute this policy.

3.6.7 Policy Statements

a. KCG provisioned email shall be used for official purposes only.
b. All use of email must be consistent with KCG policies and procedures of ethical conduct, safety, compliance with laws and proper business practices.
c. The KCG email system shall not be used for the creation or distribution of any disruptive or offensive messages. Employees who receive any emails with this content from any KCG employee should report the matter to their line manager.
d. Users are prohibited from automatically forwarding KCG email to third party email system. Individual messages which are forwarded by the user must not contain KCG Government confidential or offensive messages.
e. Emails shall be private but can be accessed if legal notice is served.
f. Emails and mail servers shall be backed up as highly mission critical services.
g. Emails and mail servers shall be afforded high availability on the Disaster Recovery and Business Continuity plan.
h. It is the responsibility of the Technical Authority to verify the emails and email server at least once per month. It is also their responsibility to report to the Executive Authority at least once per quarter.

3.6.8 General Directives on Use of KCG provided e-Mail System:

Electronic mail or "e-mail" systems are important alternative means of communication. In certain business functions, e-mail is preferred more than other conventional methods of communications. When using the KCG e-mail system the following general considerations apply:

- Minimize Messages - For KCG provided e-mail accounts, employees should minimize the number of messages in their e-mail in-box to ensure efficient function of the e-mail system.
- Maintenance of Messages - Garbage messages should be deleted regularly.
- Folders should be set up and messages filed accordingly.
- Archiving and storing - Employees should utilize the archiving facility within the e-mail system in accordance with allowed storage capacity and guidelines.

- Accounts and passwords - A register of e-mail accounts and passwords updated regularly shall be maintained by ICT department.
- Password and account expiration - It is mandatory to change e-mail passwords every 30 days or as necessary. The e-mail accounts of employees separated from the KCG shall be processed and deleted upon approval of Senior Management.
- Password security – Users should safeguard their electronic identity. Sharing of password, for example, is prohibited.

3.6.9 Email Signature

It is good email practice to make clear who the email is coming from and to include contact details in any signature so that people can get in contact with you or your section easily. This is true if you are sending an email from your own email account or emailing from the section or departmental email account.

Providing details in the email signature is important to the recipient, so that they can have easy reference to all senders' contact details.

Kisii County Government email signature should have the following standards:

1. E-mail signatures should not be longer than 10 lines. Go wider rather than longer, and use pipes (|) to separate components. Use two spaces between content and pipes.
2. Do not use images or logos within the e-mail signature.
3. Refraining from the use of quotes or epigraphs is best practice for professional communications.
4. Use a simple 12-point standard font (preferred) or your e-mail client's default font.
5. Standard E-mail Signature Format:

Name
Title
Department/Section
Kisii County Government
Office and Personal Contacts

3.6.10 Email disclaimer

The County Government of Kisii, the sender, or both can be made liable for the content of an email. A disclaimer has to be made available and should be used to protect the County and those sending emails on its behalf.

The County Government of Kisii, should use an email disclaimer to help fend off potential claims and to inform recipients of KCG's position in relation to the information being emailed. It is mandatory for all KCG employees to add a reference to the stated legal disclaimer at the bottom of their email signature.

Kisii County Government email disclaimer should have the following standards:

1. The disclaimer statement should be as specific as possible, since this will add to the weight of the statement.
2. The disclaimer should warn that the content of the e-mail is confidential.

3. The disclaimer should indicate that the message is only intended for the addressee, and that if anyone receives the e-mail by mistake they are bound to confidentiality

The following disclaimer will be added to each outgoing e-mail:

'This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this e-mail in error please notify your system manager. Please note that views or opinions presented in this e-mail are solely those of the author and do not necessarily represent those of the Kisii County Government. Finally, the recipient should check this e-mail and any attachments for the presence of viruses. The Kisii County Government accepts no liability for any damage caused by any virus transmitted by this e-mail.'

3.6.11 Email Auto Responder Standards

When out of the office and unreachable by email, all Kisii County Government employees should set up an out-of-office message to inform those seeking to contact them that they will not be in a position to respond since the employer has limited access to the email.

The email auto responder must contain:

i. The dates you will be out of the office and unreachable
ii. Any alternate forms of contacting you, if applicable
iii. The date you will be back in the office or answering emails again
iv. Information regarding an alternate contact in your office for matters requiring immediate attention

3.6.12 Limitations on Personal Use

Very limited use of KCG provided e-mail system for personal use is permitted. However, Responsible Director should ensure that there is no abuse of this privilege. Personal use of KCG e-Mail account may only occur under the following circumstances:

- Use and access only during work breaks or after office hours,
- Personal use of e-mail should not interfere with work.
- Personal e-mails must adhere to the guidelines in this standard.
- Personal e-mails must be kept in a separate folder, named 'Private'. The e- mails in this folder must be deleted monthly so as not to clog up the system.
- The forwarding of chain letters, junk mail, jokes and executable files is strictly prohibited.
- Mass mailing is strictly prohibited.
- All messages distributed via the KCG e-mail system, even personal e- mails, are KCG property.

3.6.13 Email Guidelines

3.6.13.1 Addressing

a. Email should be sent to the people who are required to either take further action or need to know the information that is being sent.

b. The “To” field should be used only for those people who are required to take further action.
c. The “Cc” field should be used for those people who only need to know the information but are not required to undertake further action.
d. The “Reply All” button should only be used when everyone in the email need to know the response.

3.6.13.2 Subject Line

a. Make sure the subject line is clear and is an accurate representation of what the email is about.
b. When conducting a conversation by email, change the subject to reflect the content of the response done.
c. Use flags to indicate whether the message is of “High Importance” or “Low Importance”.

3.6.13.3 Structure, Grammar and Tone of the Message

a. Use plain English.
b. Be polite.
c. Use paragraphs to avoid large blocks of text.
d. Avoid using “text speak” e.g. l8r instead of later.
e. Avoid using emoticons.
f. Avoid using abbreviations unless everyone being sent the message understands this or if the abbreviation has been explained in a previous message or in the message you are about to send.
g. Check the spelling and grammar before you send the email.

3.6.14 Email content

a. Always fill in the subject line with a topic that means something to the reader.
b. The main point of should be captured in the opening sentence of the email.
c. The email sender must always specify what he/she is writing about.
d. Be brief *and* polite. If your message runs longer than two or three short paragraphs, consider:
    i. Reducing the message
    ii. Providing an attachment
e. Reply promptly to serious messages. If it requires that the recipient has to take more than 24 hours to collect information or make a decision, it is important to acknowledge receipt and a communication for delay.

3.7 ICT Training Policy

Document:	Document No.:	Revision:	Effective:
Policy	KCG IT-007	1.00	[Signed Effective Date]

3.7.1 Administrative Use

This ICT Policy document seeks to provide guidelines for capacity building to give staff the required training on how to make competent use of information communication technology in the County.

This policy describes the ICT training procedure to be used by the Kisii County Government. It should be acknowledged and executed by the Director ICT.

3.7.2 Normative References

Proposed Abridged ICT Standards for GoK

IT personnel training IO/MOI/002 - This standard addresses personnel training as a means of achieving strategic objectives

IT personnel qualifications IO/MOI/001 – This standard addresses the issue of skills management and management of human resource gaps in an ICT department.

3.7.3 Purpose

To identify the process and methods taken by the County Government when conducting and/or procuring training either for the IT department or IT users in order to enhance awareness on the effective use of ICT in communications and general operations in the county.

3.7.4 Scope

This Policy applies to all training of systems and IT competencies that will require any form of assistance from the IT department. This Policy only applies to training that is under the jurisdiction and knowledge of the Director ICT.

All Kisii County Government employees are expected to adhere to it. The document shall be effective from the date of approval.

3.7.5 Consequences

The IT department shall not be held liable for any IT systems deployed without their prior knowledge or training.

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may include the offender being denied access to computing facilities.

a. Training Equipment:
   All training equipment should not be personalized in terms of setting individual passwords and making unauthorized installations of software.

b. Training materials
   Any training materials used are the property of the Kisii County Government and should not be shared outside the County fraternity. They should be kept confidentially in the custody of the person in charge of the ICT library.

3.7.6 Objective

The broad goals of this policy are:

- Establish IT training through an identified need
- Prevent the implementation/rollout of systems without the necessary training

3.7.6.1 Definitions

The following forms of training are deemed operationally necessary by the county government management and are therefore subject to this Policy:

[*Note: This section attempts to classify the applications, databases, and data structures in use in your facility. Identify them here. Deputy Director ICT to specify more detail*]

Training	Grade
Certification	A
Seminar	B
Informational	C
...[more]	...[more]

3.7.7 Responsibility and Authority

It is the responsibility of the _____(*executive authority*) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted. It is the responsibility of the Director ICT *(technical authority)* necessary to execute this Policy.

3.7.8 Policy Statements

a. Training will be performed on a basis deemed necessary to guarantee the effective support of IT systems.
b. The training shall be approved by the Deputy Director ICT and/or the requisite line manager.
c. For effective IT assistance on any system, there shall need to be an insistence on a training that is beyond Grade B that occurred for more than a single day.
d. Training durations shall be recognized as follows:

    1. Day (couple of hours)
    2. Day (Morning/Afternoon session).
    3. Days (More than 1 day).
    4. Week (More than 1 week).
    5. Month (More than 1 month).

e. It is the responsibility of the Technical Authority to keep track of the training schedule at least once per month. It is also their responsibility to provide evidence of successful completion to the Executive Authority at least once per quarter.

3.8 ICT Use Policy

Document: Policy	Document No.: KCG IT-008	Revision: 1.00	Effective: [Signed Effective Date]

3.8.1 Introduction

All Users will be lawful, efficient, economical and ethical in their use of the Kisii County Government Resources, which are provided to enable government business continuity.

3.8.2 Purpose

- Ensure ICT resources are used effectively and in a way that complies with legal and ethical standards and standards of interpersonal interaction.
- The security of departmental ICT resources is maintained.
- Safeguard Internet resources, such as e-mail and the Internet, are used appropriately.
- Ensure Copyright and intellectual property are respected.
- Enable users to understand their responsibilities in relation to the department's ICT resources.

3.8.3 ICT Resources

All of the Government's Information and Communication Technology Resources and facilities including, but not limited to: mail, telephones, mobile phones, voice mail, SMS, facsimile machines, email, the intranet, e-Services, computers, printers, scanners, access labs or other facilities that the Government owns or uses under License or by agreement, any off government computers and associated peripherals and equipment provided for the purpose of government work or associated activities, or any connection to the Government's network, or use of any part of the Government's network to access other networks.

3.8.4 User/s

All government employees, including casual employees, permanent employees and any person in any unit of the Government, including members of the general public, who have been granted access to, and use of, the Government ICT Resources.
A member of the public reading public Government web pages from outside the Government is not by virtue of that activity alone considered to be a User.

3.8.5 Conditions of Use

Use of the Government's ICT Resources is restricted to legitimate Government Business purposes only. Staff usage will depend on the nature of their work. The use of Government ICT Resources through non-government (including personally owned) equipment is also subject to this policy.

The Government will not tolerate its ICT Resources being used in a manner that is harassing, discriminatory, abusive, rude, insulting, threatening, obscene or otherwise inappropriate.
It is illegal to use any ICT Resource to harass, menace, defame, libel, vilify, or discriminate against any other person within or beyond the University. It is important to understand that in matters of discrimination and harassment it is the reasonable perception of the recipient and not the intention of the sender that is significant.

Users may be individually liable if they aid and abet others who discriminate against, harass or vilify colleagues or any member of the public. Users who adversely affect the reputation of another person may be sued for defamation by that aggrieved person.

Users must not use the Government's ICT Resources to collect, use or disclose personal information in ways that breach the Government's Privacy Policy.

Users must respect and protect the privacy of others.

Users are forbidden to use ICT Resources to access, store or transmit pornographic material of any sort other than with specific written approval from an authorized Government Officer for research related purposes.

The use of ICT Resources for gambling purposes is forbidden.

The Government forbids the use of its ICT resources in a manner that constitutes an infringement of copyright. The law permits copying and/or printing only with the permission of the copyright owner, with a few very limited exceptions such as fair use for study or research purposes (this exception itself is subject to numerous

3.8.6 Software/Hardware Policy

3.8.6.1 Purpose

The presence of a standard policy regarding the use of software and hardware will:

a) Enhance the uniform performance of the ICT Department in delivering, implementing, and maintaining software and hardware suitable to the business needs of the County Government.
b) Define the duties and responsibilities of Government employees who use various software and hardware in the performance of their job duties.
c) Facilitate the efficient use of Kisii County Government Resources.
d) Maintain software standards, ensuring compatibility between departments

3.8.6.2 Acceptable use

This section defines what constitutes "acceptable use" of the County Government's electronic resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by the county Government are to be used only for creating, researching, and processing government-related materials, and other tasks necessary for discharging one's employment duties.

By using Kisii County Government hardware, software, and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable company policies, as well as city, state, and federal laws and regulations.

3.8.7 Enforcement

Failure to observe these guidelines may result in disciplinary action by the county Government depending upon the type and severity of the violation, whether it causes any liability or loss to the Government, and/or the presence of any repeated violation(s).

3.8.8 Definitions

3.8.8.1 Software

Any program, or feature requiring set-up or installation of any type. This definition includes but not limited to programs, feature enhancements, upgrades, add-ins, clip-art etc. This also includes purchased items subject to any licensing agreement, shareware, or items distributed for free.

3.8.8.2 Hardware

The system unit, monitor, keyboard, mouse, and any other additional peripherals such as printers, scanners, modem or video capture device.

3.8.9 Administration

The ICT Director is responsible for the administration of this policy. This policy is a living document and may be modified and reviewed due to the different technological changes experienced every day.

3.8.10 Software

All software acquired for or on behalf of the Kisii County Government or developed by Kisii County Government employees or contract personnel on behalf of the government is and at all times shall remain company property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

3.8.11 Purchasing

All purchasing of Kisii County Government software shall be centralized within the ICT Department to ensure that all applications conform to corporate software standards and are purchased at the best possible price. All requests for corporate software must be submitted to the department Director for his/her approval. The request must then be reviewed to ascertain the need for such software, and then determine the standard software that best accommodates the desired request.

3.8.12 Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on government computers. If an employee needs help in interpreting the meaning/application of any such licenses, notices, contracts and agreements, he/she will contact the ICT Department for assistance.

3.8.13 Software standards

The following list shows the standard suite of software installed on government computers (excluding test computers) that is fully supported by the information technology department:

- Microsoft Windows 7
- Microsoft Outlook
- Microsoft Office (Word, Excel, PowerPoint, Access, Photo Editor)
- Microsoft Internet Explorer
- Microsoft AntiSpyWare
- Adobe Acrobat Reader

- WinZip
- Media Player, Real Player, QuickTime
- CD Writing Software
- Acronis

Where applicable the following software will be installed on the county government computers

- Microsoft Visio
- Microsoft Project
- Microsoft Publisher
- Dreamweaver
- PageMaker

Employees needing software other than those programs listed above must request such software from the ICT department. Each request will be considered on a case-by-case basis in conjunction with the software-purchasing section of this policy.

3.8.14 Software Installation

The ICT department is exclusively responsible for installing and supporting all software on Kisii County Government computers. These responsibilities extend to:

a) Office desktop computers
b) Company laptop computers
c) Computer lab desktop computers

The ICT department relies on installation and support to provide software and hardware in good operating condition to the employees so that they can best accomplish their tasks.

3.8.15 Hardware

All hardware devices acquired by the ICT Department or developed by it (through its own employees or through those hired to develop the hardware devices) is and at all times shall remain the government property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

3.8.16 Purchasing

All purchasing of computer hardware devices shall be centralized to ensure that all equipment conforms to corporate hardware standards and is purchased or leased at the best possible price.

All requests for corporate computing hardware devices must be in the annual corporate budget document and have the department Directors approval. The request must then be reviewed to establish the need for such hardware, and then determine standard hardware that best accommodates the desired request.

3.8.17 Hardware standards

The following list shows the typical minimum hardware configuration for new Kisii County Government computers:

3.8.17.1 Desktops; provided to employees who work primarily from the office.

- ✓ Intel Processor or AMD
- ✓ 4GB RAM
- ✓ Windows 7 Professional
- ✓ Integrated Video
- ✓ 1.44M 3 ½" floppy drive
- ✓ 160GB hard drive
- ✓ 24X CDRW/DVD
- ✓ Integrated 10/100/1000 Ethernet
- ✓ Integrated Audio
- ✓ Speakers
- ✓ USB Enhanced Multimedia Keyboard
- ✓ USB Optical Mouse with Scroll
- ✓ All applicable cables
- ✓ Surge protector
- ✓ 3 year warranty / 3 year onsite service

3.8.17.2 Laptops; provided to employees required to frequently work away from the office.

- ✓ Speed - 1.8 GHz
- ✓ 4 GB RAM
- ✓ 32 MB Video Adapter
- ✓ 1.44M 3 ½" floppy drive
- ✓ 500 GB IDE hard drive
- ✓ 24X Combo DVD/CDRW
- ✓ Integrated 10/100 Ethernet
- ✓ Integrated Wireless
- ✓ Integrated 56K modem
- ✓ 2 USB port
- ✓ Integrated Audio
- ✓ Docking station / Port Replicator
- ✓ Speakers
- ✓ Surge protector
- ✓ Carrying case
- ✓ Extra power adapter and mouse
- ✓ 3 year warranty / 3 year onsite service

3.8.17.3 Monitors

- ✓ Monitors will be provided for desktop systems.
- ✓ Minimum 17" ***viewing*** area, 1024 x 768

3.8.17.4 Printers

- ✓ Employees will be given access to appropriate network printers. In some limited cases, employees may be given local printers if deemed necessary by the department director in consultation with the ICT department.
- ✓ Employees needing computer hardware other than what is stated above must request such hardware from the ICT department. Each request will be considered on a case-by-case basis in conjunction with the hardware-purchasing section of this policy.

3.8.17.5 outside equipment

No outside equipment may be plugged into the Kisii County Government's network without the ICT department's written permission.

3.9 Internet Policy

Document:	Document No.:	Revision:	Effective:
Policy	KCG IT-009	1.00	[Signed Effective Date]

3.9.1 Overview

Internet connectivity presents Kisii County Government with new risks that must be addressed to safeguard vital information assets. These risks include:

- Access to the Internet by personnel that is inconsistent with county governments needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the county government may face loss of reputation and possible legal action through other types of misuse.
- All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

An internet usage policy provides employees with rules and guidelines about the appropriate use of Kisii County government equipment, network and Internet access. Having such a policy in place helps to protect both the county government and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to or there could be serious repercussions, thus leading to fewer security risks for the county government as a result of employee negligence.

The Internet Usage Policy is an important document that must be signed by all employees upon starting work.

3.9.2 Normative References

Proposed Abridged ICT Standards for GoK

Internet traffic Monitoring N/I/003 – This standard applies to all end user initiated communications between network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols.

Internet Access N/I/002 - This standard ensures that the access policy is adhered to.

3.9.3 Purpose

To define policies and procedures for access to the Internet through Kisii County Government network infrastructure.

3.9.4 Scope

The Internet usage Policy applies to all Internet users (individuals working for the Kisii County Government, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The county's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

3.9.5 Objectives;

The broad goals of this policy are:

a. Minimize security risks for Kisii County government internet resources as a result of employee negligence
b. Prevention of misuse of County Government internet resource

3.9.6 Responsibilities and Authority

Kisii County Government users are responsible for:

a. Honoring acceptable use policies of networks accessed through County Internet and e-mail services.
b. Abiding by existing federal, state, and local telecommunications and networking laws and regulations.
c. Following copyright laws regarding protected commercial software or intellectual property.
d. Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of County's network resources.
e. Using logical, professional, ethical and other applicable laws, guidelines and procedures to maintain the security of sensitive information.

3.9.7 Policy Statements

3.9.7.1 Personal Use

Kisii County government recognizes that its employees and clients may need to use these county internet facilities for reasonable private use. However, private use of Internet facilities should never interfere with the duties and functions of the employee or Kisii county government technical infrastructure.

3.9.7.2 Acceptable Usage

Internet usage is granted for the sole purpose of supporting county activities necessary to carry out job functions. All users must follow the government principles regarding resource usage and exercise good judgment in using the Internet.

Acceptable use of the Internet for performing job functions might include:

a. Communication between employees and non-employees for business purposes;
b. IT technical support downloading software upgrades and patches;
c. Review of possible vendor web sites for product information;
d. Reference regulatory or technical information.
e. Research

3.9.7.3 Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited

The county government also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing county government information that is not within the scope of one's work. This includes unauthorized reading of personnel account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering personnel information. This includes making unauthorized changes to a personnel file or sharing electronic personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of county government Web sites to other Internet/www sites whose content may be inconsistent with or in violation of the aims or policies of the county government.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
- Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

3.9.7.4Software License

Kisii County government strongly supports strict adherence to software vendors' license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

3.9.7.5 Maintaining County Government Image

3.9.7.5.1 Representation

When using county government's resources to access and use the Internet, users must realize they represent the county. Whenever employees state an affiliation to the county, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Kisii County Government". Questions may be addressed to the IT Department.

3.9.7.5.2 County Government Materials

Users must not place county government's material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service without approval from the communications department

3.9.8 Internet traffic monitoring

3.9.8.1 Rationale

These standards are designed to ensure Personnel use the Internet in a safe and responsible manner, and ensure that personnel web use can be monitored or researched during an incident.

3.9.8.2 Brief description of standard

The Government should establish a policy to define standards for systems that monitor and limit web use from any host within network.
This standard makes the assumption that roles and responsibilities are clearly defined, communicated and understood by all personnel.

This standard applies to all end user initiated communications between network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols.

3.9.9 Internet Access

3.9.9.1 Rationale

There is need to maintain the security of information. This is implemented by use of firewalls and proxies as per the access policy.

3.9.9.2 Brief description of standard

The Government should ensure that access to the Internet from Government information technology service information resources are routed through Government information technology Service-approved access control technology (e.g., firewalls and proxies). This standard ensures that the access policy is adhered to.

3.10 Password Policy

Document: Policy	Document No.: KCG IT-010	Revision: 1.00	Effective: [Signed Effective Date]

3.10.1 Overview

This policy describes the password procedure to be used by the Kisii County Government. Passwords are an important aspect of computer security. They are the front line of protection for user accounts and a gateway to accessing various resources on different machines. A poorly chosen password may result in the compromise of the county Government's entire network. As such, all government employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.10.2 County Critical Systems

The following forms of information are deemed operationally critical by the County Government management and are therefore subject to this Policy:

Critical IT System
IPPD
IFMIS/ IB
LAIFOMS
CIFMIS
Shared File System
Network Firewall (Untangle NG Firewall)
Active Directory

This policy also applies in all environments that will require the use of passwords.

3.10.3 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. This Policy applies to all of the IT systems deemed mission-critical by the County Government at all of its locations.

3.10.4 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Kisii County Government facility, has access to the network, or stores any non-public government information.

3.10.5 Policy Statements

a. All system-level passwords must be changed on at least a quarterly basis.
b. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every month
c. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
d. Passwords must not be inserted into email messages or other forms of electronic communication.

e. All user-level and system-level passwords must conform to the guidelines described below.

3.10.6 Guidelines

3.10.6.1 General Password Construction Guidelines

Passwords are used for various purposes at Kisii County Government. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software. The words "COUNTY", "kcg", "kisii" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, QWERTY, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9,!@#$ %^&*() _+|- =\` {} [] :";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "One way I can remember my password" and the password could be: "Ow1crMp#" or "1Wic? mp/" or some other variation.

3.10.6.2 Password Protection Standards

a. Do not use the same password for Kisii County Government accounts as for other non-government access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various government access needs. Do not share government passwords with anyone, including administrative assistants or secretaries.
b. All passwords are to be treated as sensitive, confidential government information.
c. Here is a list of "don’ts":
d. Don't reveal a password over the phone to ANYONE
e. Don't reveal a password in an email message
f. Don't reveal a password to your supervisor

g. Don't talk about a password in front of others
h. Don't hint at the format of a password (e.g., "my family name")
i. Don't reveal a password on questionnaires or security forms
j. Don't share a password with family members
k. Don't reveal a password to co-workers while on vacation
l. If someone demands a password, refer them to this document or have them call someone in the Information Technology (IT).
m. Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, Instant Messenger, or any other application).
n. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
o. Change passwords at least once every months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.
p. If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

3.10.6.3 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

3.10.6.3.1 Applications:

1. Should support authentication of individual users, not groups.
2. Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

3.10.6.4 Remote Access

Access to the Kisii County Networks via remote access is controlled using Cisco Virtual Private Networking (VPN). VPN client software is available from IT.

3.10.6.5 Passwords at Account Creation

When a request for a username is requested, IT staff will determine the type and privileges required as filled in the official access request form. The password will be set to be pre-expired so the user will be required to change their password when they first successfully logon to the system. The lifetime of the password will be set according to the guidelines set in section 4.1 of this document.

3.10.6.6 Forgotten Passwords

Users will occasionally forget their password. A characteristic of password files is that passwords cannot be looked up. If a user forgets their password, the password can be changed by IT staff. The user must send a request to the IT staff member before the password will be changed. Users who cannot contact IT in person on a branch campus should go to the Business Office of the branch campus to present the photo id and then the branch campus personnel will contact IT to make the password change. In the case of student Blackboard passwords, the student's instructor can make appropriate identification and change the password for the student.

3.10.7 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.11 Social Media Policy

Document:	Document No.:	Revision:	Effective:
Policy	KCG IT-011	1.00	[Signed Effective Date]

3.11.1 Administrative Use

This policy is intended to assist staff make appropriate use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, which include but not limited to Twitter, Facebook, LinkedIn, YouTube and Instagram..

This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor the use of social media and the action to be taken in respect of breaches of this policy.

This policy supplements the Internet and Email Policy.

This policy does not form part of any contract of employment and it may be amended at any time.
This policy describes the social media use by the Kisii County Government. It should be acknowledged and executed by the IT Manager.

This policy is substantively covered by the government of Kenya ICT Standards on Messaging and Collaboration. To govern communication, the government has adopted a strategic openness and agility in deployment and usage of messaging and collaboration ecosystem as it is critical to maximizing the potential of government operation in service delivery.

3.11.2 Normative References

Proposed Abridged ICT Standards for GoK
Social Media and Email – Social Media Policy MAC/SMA/001 – This standard makes the assumption that personnel and officers will not abuse social sites by being careful on what contents they post relating to affairs and matters of the Government.
This standard offers guidance on how social media can be used by staff in various MDAs while taking into considerations implications that comes along with use of social media.

3.11.3 Purpose

To identify the process and methods taken by the County Government to safeguard its image and communication over social media

3.11.4 Scope

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees,

homeworkers, part-time and fixed-term employees, students on attachment, interns, casual and agency staff and volunteers (collectively referred to as **staff** in this policy)
All staff are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of our County and our services, employees, partners, customers, the publics and competitors.

This Policy applies to all posts on official County Government social media accounts at all of its locations. This Policy only applies to acknowledged and approved County Government social media accounts, and that is under the jurisdiction and knowledge of the County ICT DIRECTOR.

3.11.5 Consequences

Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

3.11.6 Objective

The broad goals of this policy are:

- Protection of County Government speech on Social media
- Protection of data integrity and confidentiality
- Facilitate the timely and efficient posting of county activities on social media

3.11.7 Social Media Accounts

The following forms of social media are deemed operationally useful by the County Government management and are therefore subject to this Policy. The criticality is based on the perceived number of users on such social media platform. The county government shall not be held responsible for any personal social media accounts by any of its members. Members of the county government should be made aware that their personal social media accounts and whatever is posted therein shall be their sole responsibility and shall not reflect the official position of the county government. County government members shall also be educated on the sensitivity of posting on social media, as their activities reflect by association the character of the county government

Critical Social Media Platform	Grade	Account Name
Facebook	1	
Twitter	2	
Instagram	3	
Blog	4	
...[more]	...[more]	

No staff is allowed to open accounts that act as a parody to the official accounts.

3.11.8 Responsibility and Authority

The Director ICT has overall responsibility for the effective operation of this policy.
The Director ICT is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimize risks to our operations.

All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any breach of this policy should be reported to Director ICT.
Questions regarding the content or application of this policy should be directed to Director ICT.

3.11.9 Policy Statements

a. Social Media updates will be performed on a basis deemed necessary to communicate the county government mission to the members of Kisii County. Acceptable frequencies are as follows:
    - Daily (Mon-Fri).
    - Weekly (Sun).
    - Monthly (1st of every month).
    - Quarterly (1st of every quarter).
b. Social Media updates will be performed on the approved platforms by the assigned social media IT Function employee.
c. Social Media updates will be performed by Grade, on the following frequency, using the following media:

Grade	FREQUENCY	NOTES
1	Daily	
2	Weekly	
3	Monthly	

d. It is the responsibility of the Technical Authority to verify the social media updates at least once per month. It is also their responsibility to provide evidence of successful posts to the Executive Authority at least once per quarter.

3.11.10 Social Media Standards

3.11.10.1 Rationale

Use of email and social media in the Government will encourage members to engage, build networks of like-minded people in certain fields of expertise, stay connected, share information and help promote the Government's goals and vision in an effective and cheaper way.

3.11.10.2 Brief description of standard MAC/SMA/001

This standard makes the assumption that personnel and officers will not abuse social sites by being careful on what contents they post relating to affairs and matters of the Government.
This standard offer guidance on how social media can be used by staff in various MDAs while taking into considerations implications that comes along with use of social media.

3.11.11 Social Media Acceptable Use

3.11.11.1 Rationale

Use of social media for communication purposes in the Government should be governed to ensure that their use is suitable for business purposes that support the goals and objectives of the Government of Kenya and its ministries and departments.

3.11.11.2 Brief description of standard MAC/SMA/002

The Government of Kenya recognizes that the principles of freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services and the social media. However, this is subject to standards that enhance proper use of these resources to limit abuse and possible litigations that may arise through actions taken by Government personnel using these facilities.
This standard makes the assumption that personnel will follow the laid down guidelines to ensure acceptable use of email and social media.
This standard defines the acceptable usage of government communication resources.

3.11.12 Social Media Guidelines

a. Using social media sites in our name
   - ✓ Only the IT Officer are permitted to post material on a social media website in our name and on our behalf. Any breach of this restriction will amount to gross misconduct.

b. Requirements / Expectations
   - ✓ These are rules that apply to all communications made by you in your capacity as our employee or which in any way relate to our services.
   - ✓ All communications we make using social media which promote our services can only be made by Communications Officer and must have been through our formal approval process.
   - ✓ Otherwise, you must not make any communication using social media which undermine our County and its services.
     Any breach of these restrictions will amount to gross misconduct.
   - ✓ If you are in any doubt as to what you can and cannot say using social media, then please contact Director ICT.

c. Using work-related social media
   - ✓ We recognize the importance of the internet in shaping public thinking about our county and our services, employees, partners and customers. We also recognize the importance of our staff joining in and helping shape county conversation and direction through interaction in social media.
   - ✓ You are therefore permitted to interact on [approved] social media websites about industry developments and regulatory issues. Approved social media websites are:
     - ➢ Facebook
     - ➢ Twitter
     - ➢ Instagram

     This list may be updated by the Director ICT.
   - ✓ Before using work-related social media you must:

- Have read and understood this policy, the Communications Policy and the Internet and Email Policy; and
- Have sought and gained prior written approval to do so from Director ICT.

d. Personal use of social media sites

- ✓ We permit the incidental use of social media websites for personal use subject to certain conditions set out below. However, this is a privilege and not a right. It must neither be abused nor overused and we reserve the right to withdraw our permission at any time at our entire discretion.
- ✓ The following conditions must be met for personal use to continue:
  - use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm);
  - Use must not breach any of the rules set out in paragraph 9 below.
  - use must not interfere with business or office commitments;
  - Use must comply with our policies including the Internet and Email Policy, Data Protection Policy and Disciplinary Procedure.

e. Rules for use of social media

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules:

- ✓ Always write in the first person, identify who you are and what your role is, and use the following disclaimer "*The views expressed are my own and don't reflect the views of my employer*".
- ✓ Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- ✓ Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Human Resources Manager.
- ✓ Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with Human Resources Manager.
- ✓ Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.
- ✓ It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticizing it. However, if you think an excerpt is too big, it probably is. Quote accurately, include references and when in doubt, link, don't copy.
- ✓ Before you include a link to a third party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.
- ✓ When making use of any social media platform, you must read and comply with its terms of use.

- ✓ Do not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.
- ✓ Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of us as a County. If you make a mistake in a contribution, be prompt in admitting and correcting it.
- ✓ You are personally responsible for content you publish into social media tools – be aware that what you publish will be public for many years.
- ✓ Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.
- ✓ If you feel even slightly uneasy about something you are about to publish, then you shouldn't do it. If in doubt, always discuss it with the Director ICT first.
- ✓ Don't discuss colleagues, competitors, customers or suppliers without their prior approval.
- ✓ Always consider others' privacy and avoid discussing topics that may be inflammatory that may amount to hate speech.
- ✓ Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details.
- ✓ Before your first contribution on any social media site, observe the activity on the site for a while before launching in yourself to get a feel for the style of contributions, the nature of the content and any 'unwritten' rules that other contributors might follow.
- ✓ Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.
- ✓ If you notice any content posted on social media about us (whether complementary or critical) please report it to the Director ICT.

f. Monitoring use of social media websites

- ✓ Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under our Disciplinary Procedure.
- ✓ We reserve the right to restrict or prevent access to certain social media websites if we consider personal use to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.
- ✓ Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and us. It may also cause embarrassment to us and to our clients.
- ✓ In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):
    - pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
    - a false and defamatory statement about any person or organization;

- material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our clients or our staff;
- confidential information about us or any of our staff or clients (which you do not have express authority to disseminate);
- any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
- Material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.
- Any such action will be addressed under the Disciplinary Procedure and is likely to result in summary dismissal.

✓ Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary such information may be handed to the police in connection with a criminal investigation.

✓ If you notice any use of social media by other members of staff in breach of this policy please report it to Director ICT and/or Human Resources Manager.

3.12 Server Security Policy

Document: Policy	Document No.: KCG IT-012	Revision: 1.00	Effective: [Signed Effective Date]

3.12.1 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Kisii County. Effective implementation of this policy will minimize unauthorized access to Kisii county Government proprietary information and technology.

3.12.2 Scope

This policy applies to server equipment owned and/or operated by Kisii County Government, and to servers registered under any Kisii county government-owned internal network domain.

It is specifically for equipment on the internal Kisii County Government network. For secure configuration of equipment external to KCG on the DMZ.

3.12.3 Ownership and Responsibilities

a. All internal servers deployed at Kisii County Government must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the Director ICT. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a

process for changing the configuration guides, which includes review and approval by ICT.

b. Servers must be registered with ICT. At a minimum, the following information is required to positively identify the point of contact:
   i. Server contact(s) and location, and a backup contact
   ii. Hardware and Operating System/Version
   iii. Main functions and applications, if applicable
c. Information in ICT must be kept up-to-date.
d. Configuration changes for production servers must follow the appropriate change management procedures.

3.12.4 General Configuration Guidelines

a. Operating System configuration should be in accordance with approved ICT guidelines.
b. Services and applications that will not be used must be disabled where practical.
c. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
d. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
e. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is available.
f. Always use standard security principles of least required access to perform a function.
g. Do not use root, or administrative accounts when a non-privileged account is sufficient.
h. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).
i. Servers should be physically located in an access-controlled environment.
j. Servers are specifically prohibited from operating from uncontrolled areas, such as personal or shared offices.

3.12.5 Monitoring

a. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
   i. All security related logs will be kept online for a minimum of 1 week.
   ii. Daily differential backups will be retained for at least 1 month.
   iii. Weekly full backups of logs will be retained for at least 1 month.
   iv. Monthly full backups will be retained for a minimum of 1 year.

b. Security-related events will be reported to ICT, who will review logs and report incidents to ICT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
   i. Port-scan attacks
   ii. Evidence of unauthorized access to privileged accounts

iii. Anomalous occurrences that are not related to specific applications on the host.

3.12.6 Compliance

a. Audits will be performed on a regular basis by authorized organizations within Kenya.
b. Audits will be managed by the internal audit group or ICT, in accordance with the *Audit Policy*. ICT will filter findings not related to a specific operational group and then present the findings to the appropriate ICTO support staff for remediation or justification.
c. Every effort will be made to prevent audits from causing operational failures or disruptions.

3.12.7 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.12.7.1 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the production network.
Server	For purposes of this policy, a Server is defined as an internal Kisii County Government Server.

NOTE: Desktop machines and Lab equipment are not relevant to the scope of this policy.

3.13 Software Development Policy

Document: Policy	Document No.: KCG IT-013	Revision: 1.00	Effective: [Signed Effective Date]

3.13.1 Administrative Use

The County Government of Kisii's System Development Policy applies equally to all individuals that use any County Information Resources.

3.13.2 Purpose

The purpose of the System Development Policy is to describe the requirements for developing and/or implementing new software in the County Government Information Resources.

3.13.3 Scope

The policy covers the Software Development Lifecycle (SDL). Moreover, the policy also covers the support required for any operational Information Systems, integrity of data, request for service, and accessibility of Information.

3.13.4 Consequences

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of

contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of County Information Resources access privileges, civil, and criminal prosecution.

3.13.5 Objectives

To stipulate practices, processes, objectives, and internal controls for software development.

3.13.6 Responsibility and Authority

It is the responsibility of the _____(*executive authority*) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted. It is the responsibility of the Systems Developer (Technical authority) to verify the practices and procedures necessary to execute this policy.

3.13.7 Policy Statements

a. The ICT department is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for the Kisii County Government system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical county information.

b. All production systems must have designated Owners and Custodians for the critical information they process. ICT department must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

c. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) must be assigned for all production systems.

d. Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.

e. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

3.13.8 Project Planning & Organization Standards

Prior to the computerization or acquisition of any County Information System, the Director of ICT shall constitute an Information System project team to sphere head the development of the systems.

a) The Director ICT shall appoint a Project Leader for every system project.
b) In case the project leader finds that there are some stakeholders that have been excluded from the project team then he or she shall make a request to the Director for them to be included.
c) The Director ICT shall ensure that each Information System Project has an organization chart.
d) The roles and responsibilities of the different persons involved in the project development and implementation shall be clearly defined in the project job description document and everyone in the project trained on them. The Director of ICT shall facilitate the drafting of this document.
e) The Project Leader shall:
    - Identify a development methodology to be used. The methodology shall address the following: requirements, design, implementation, and monitoring and evaluation (maintenance) phases.
    - Identify all the important milestones in the development cycle and indicate the expected deliverables that would include: feasibility study report, development plan, requirements document, design document, testing, implementation and change control procedures.
    - Ensure that all changes made to the system follow the change control procedures.
    - Ensure that the project has a project plan and implementation methodology.
    - Ensure that risk assessment and management procedures have been put in place.
    - Be charged with the responsibility of ensuring that the project has a software versioning mechanism and release plan, indicating the number of versions and releases expected and when they are to be out.

3.13.9 Requirements Phase

a) In this phase of software development, the Systems Analyst shall identify functional, constraint and quality (including performance, compatibility, usability and security) requirements of the envisaged system.
b) In this phase, the Project Team Leader shall review the efficiency of the processes to be computerized through re-engineering. Any recommendations that come out of the reengineering process shall be communicated to the main stakeholder (or champion) who shall be responsible for channeling them to the relevant County organs for adoption in the County.
c) At the end of the requirements phase, the Project Team Leader will present to the stakeholders a requirement specification document. The

stakeholders will then validate the document to verify that their requirements have been captured correctly in accordance with the documentation standards.

3.13.10 Design phase

The design phase shall have the following sub-phases:

a) Preliminary design phase
In this phase, the Systems Analyst in conjunction with the Project Leader shall produce a design document showing the overall design of the new system. The deliverables in this phase shall be: a design document and a user interface design document.

b) Main design phase
In this phase, the Systems Analyst in conjunction with the Project Leader shall perform detailed design of the functionality of the new system with the aim of establishing complete details of all the possible actions and results in the requirements. This phase shall cover: input/output design, file design and a logical data model of the envisaged system. The deliverable in this phase shall be a Design or Functional Specification document.

c) Review or validation phase
In this phase the Project Team Leader in consultation with the Stakeholders shall review and validate the design documents and make any changes as recommended or appropriate. The result of this phase shall be validated design documents.

3.13.11 Implementation

The Project Leader shall ensure that:

a) Systems Analysis is planned for and user training executed in the best way possible with appropriate schedules for the different categories of system users.
b) Prior to the deployment of any system (developed or procured), the system is thoroughly subjected to tests including but not limited to, unit, integration, system, volume, usability, acceptance and performance testing
c) The project has ready and up to standard documentation before handover to the stakeholders.
d) System changeover is planned for and executed using the best technique that will have minimum negative impact on the user operations.

3.13.12 Monitoring and evaluation

a) The Project Team Leader will have to put in place modalities for ensuring that the system developed is reviewed after every six months or such a time deemed fit to find out if the System is still fulfilling the user requirements, and if not, appropriate actions taken to ensure that the System meets the ever changing user needs.

b) A system that is too costly to maintain, does not meet user requirements or is deemed to be obsolete shall be retired after consultation with all stakeholders.
c) Any changes in any system shall be done through the change control procedure.

3.13.13 Guidelines

This guideline provides specific guidance on the use and management of requirements. They apply when an information system or service is being developed, modified or procured by, or on behalf of, the County Government of Kisii.

1. SDLC Documentation

Develop and maintain a well-documented SDLC for all system and application development processes. At a minimum, the SDLC documentation will include:

a) Project initiation (planning);
b) Requirements definition (analysis);
c) System design;
d) System development;
e) Testing;
f) Implementation and support;

2. SDLC Management and Controls

Ensure adequate SDLC management processes and controls exist. Essential management processes and controls over the system development (project) process include:

a) Appropriate strategic planning for projects within the IT short-and long-term plans, including authorization and reporting requirements from senior management to the board
b) Periodic reporting to the board on project status and target completion dates (including budget variance reports);
c) Requirements for internal audit involvement in mission critical projects;
d) Requirements for security officer/team involvement regarding security controls.

3. Change Control Approval

Document standards for managing change to an existing information systems infrastructure. The Change Control process includes:

a) Management and business unit approval of the change request;
b) Specification of change;
c) Approval for access to source code;
d) Programmer completion of change;
e) Request and approval to move source code into the test environment;
f) Completion of acceptance testing by business unit owner;
g) Request and approval for compilation and move to production;
h) Determination and acceptance of overall and specific security impact.

4. Change Control Documentation

Document the process for modifying information systems programs. Change Control documentation includes:

a) Change request date;
b) Person(s) requesting;
c) Change request approval;
d) Change request approval and acceptance (Management and business users);
e) Documentation revision date;
f) Quality assurance approval;
g) Final business unit owner acceptance and approval;
h) Date moved into production.

5. Testing Standards

Document testing standards and procedures. Standard testing procedures include:

a) A documented test plan;
b) Types of tests to be used (e.g., unit, parallel, user test, regression);
c) A restriction of the use of live files in testing to prevent destruction or alteration of live data;
d) Simulated error conditions to ensure that the program effectively handles all situations;
e) Independent verification, documentation, and retention of test results.

6. Requirement Practices

a) Known requirements and constraints MUST be documented.
b) Known assumptions MUST be documented.
c) Known uncertainties MUST be documented to ensure that proof of concept projects have focused, tangible objectives.
d) The documentation from items 1-3 above SHOULD be peer reviewed for completeness and clarity of purpose by one or more people qualified to provide constructive feedback on completeness and clarity of purpose, but who have not directly participated in producing the documents.
e) Requirements and constraints MUST be subjected to an approval process. The source of a requirement should be documented.
f) Final design and implementation choices MUST be based on approved requirements/constraints.

7. Properties of Requirements

a) Each requirement MUST be testable against objective criteria. If a requirement is not verifiable by some objective criteria, then there is no way to validate that the requirement has been satisfied or otherwise delivered.
b) Each requirement SHOULD be specific: free of ambiguity and not open to unconstrained interpretation.
c) A requirement SHOULD NOT arbitrarily restrict solution choices.

d) Each requirement MUST be uniquely identified. Once assigned a unique identifier should be persistent, i.e. the identifier should never be reused or reassigned even if the requirement itself is dropped.
e) A requirement statement SHOULD express only one requirement, not more. A requirements statement, i.e. a sentence, should express one coherent requirement, not a multitude of requirements.

3.14 ICT Technical Assistance Request Policy (KCG IT-008)

Document: Policy	Document No.: KCG IT-014	Revision: 1.00	Effective: [Signed Effective Date]

3.14.1 Administrative Use

This policy describes the IT Technical Assistance procedure to be used by the Kisii County Government. It should be acknowledged and executed by the IT Manager.

3.14.2 Normative References

Proposed Abridged ICT Standards for GoK

1. Incident Management IO/BC/003 – This standard addresses incident management and service operation restoration.

3.14.3 Purpose

To identify the process and methods taken by the County Government's IT Help Desk to safeguard smooth operations at the county offices.

3.14.4 Scope

This Policy applies to all of the help desk assistance calls by the County Government officers to the IT department. This Policy shall apply to all requests for the utilization of any ICT human resource.

3.14.5 Consequences

Assistance requests that are not in line with the laid down policy shall not be processed

3.14.6 Objective

The broad goals of this policy are:

- Establishment of an SLA by the IT department with all other departments in the county government
- Classification of Assistance requests based on urgency

3.14.7 Responsibility and Authority

It is the responsibility of the_____ (*executive authority*) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted. It is the responsibility of ICT DIRECTOR (*Technical authority*) to verify the practices and procedures necessary to execute this Policy.

3.14.8 Policy Statements

a. An SLA, physical or salient shall be maintained between the IT department and other departments within the county government based on (criticality, importance, etc.):
b. Every request for assistance shall be logged centrally through a ticketing solution and assigned to an IT department helpdesk resource.
c. Ticket shall be treated according to the SLAs:
d. It is the responsibility of the Technical helpdesk ICTO to verify that all the tickets are closed at least once per month. It is also their responsibility to provide evidence of successful assistance to the Executive Authority at least once per quarter.

3.14.9 Service Level Agreement

3.14.9.1 Service Framework

The ICT department has adopted the industry best practice ITIL support framework to underpin its service support and delivery. A number of ITIL elements are used, including incident management, problem management, configuration, change and release management and service level management.

3.14.9.2 Support Objectives

- To meet the changing needs of County IT users
- To provide high service availability and resilience compatible with cost effective operations
- To ensure that all staff and students using County computing resources are adequately supported and assisted in their day to day activities
- To ensure that users clearly understand what level of service to expect and their own obligations to provision of these services
- To respect and safeguard confidentiality of data and equipment
- To consult on the services with Departments via Departmental Representatives and other mechanisms

3.14.10 ICT Department Responsibilities

ICT department will:

a. Take responsibility for provision of the IT infrastructure, e.g. servers, LAN, WAN and Internet connections. Infrastructure is set up where possible in a resilient manner so that it is to be available at all times. Support is only available during normal business hours (08.00 – 17.00) on county working days; out of hours support is available for some key services; see 2.6.4
b. Ensure access to the Central Service Desk within advertised hours.
c. Support a range of supported hardware and software agreed with our users. This range will be reviewed on an annual basis.
d. Equipment outside the range will be covered on a reasonable endeavors basis only.
e. reserve the right to take systems out of service for upgrades and other changes if necessary publicize the proposed downtimes for all services for users' reference
f. provide 1 week advance notice of planned outages outside a regular system maintenance period (see below)

g. Inform Department heads and other users likely to be affected by serious faults affecting services.
h. Ensure that changes to major county IT services will go through the ICT change management process
i. offer only limited support for machines or software where there is no current maintenance contract or warranty agreement
j. Provide systems and services in accordance with the County IT Security Policy.
k. Ensure that all support activity is completed within public Health and Safety requirements.
l. undertake regular software audits of County computer systems to ensure compliance with software licensing policies
m. ensure that services and support comply with the County Sustainability Policy
n. seek the agreement of the user before connecting to their computer remotely to diagnose or fix faults

3.14.11 ICT User Responsibilities

ICT Users will:

a. follow the appropriate procedures for contacting the Service Desk in order to receive the levels of service specified in this document
b. when requesting services from ICT, provide a named contact who has the necessary authority to make decisions about the work
c. conform to County Conditions of Use and Security Policy
d. provide reasonable access (subject to County Health and Safety standards) to support staff in order for them to complete their work
e. to meet service level targets Inability to give reasonable access may result in requests being delayed or closed
f. Ensure their computers are available on the network to allow support staff remote access to diagnose and fix faults. Failure to do so may result in Support Staff taking longer to resolve issues
g. provide administration access rights to ICT staff in order to be able to update machine configurations and software as necessary
h. ensure that all computers have a nominated owner, custodian and system administrator as applicable
i. Ensure that only properly licensed software is installed on County computer equipment and correctly registered with the County.
j. machines with unlicensed software will not be supported until the software has been deleted or licensed properly
k. Make their computer available for periodic mandatory audits. These will be undertaken to ensure compliance with County software
l. Licensing policies. Systems which have not been audited in accordance with County policies will not qualify for support under this

3.14.12 Outline of Support Process

All requests for assistance should first be logged at the Service Desk which will manage the calls to resolution. Calls will be categorized as either Incidents or Service Requests (Tasks). In general, resolution of incidents takes precedence over fulfillment of Service Requests (Tasks).

3.14.12.1 Incidents

An incident is where an error or disruption to an existing service has occurred that requires resolution to enable normal working to continue. Incidents are allocated priorities according to the business impact and urgency of the situation.

3.14.12.2 Service Requests (Tasks)

These are requests for a service such as installing a new computer, providing access to a computer application or upgrading an existing PC.

3.14.13 ICT Computing Support Elements:

3.14.13.1 First line support (entry point)

The ICT Service Desk provides the first line support and they can be contacted by telephone, email, ticketing system or face to face.

3.14.13.2 Second line support

If first line support are unable to resolve the fault the call will be passed to second or third line support depending on the nature of the fault. The second line Faculty Support teams are ICT support staff based in Departments

3.14.13.3 Third line support

The third line teams include technical specialists who are responsible for development of IT Services. Third line support will resolve in-depth support issues which cannot be resolved by first and second line teams.

3.14.13.4 Normal Service Hours

Normal College business hours are 08.00 to 17.00 on working days. ICT Services are usually available during normal County business hours, except if system maintenance has been agreed. Support is available at these times via the Service Desk,

3.14.13.5 Remote Assistance

Support Staff may use remote assistance tools to connect to a customer's computer to help diagnose and fix a fault without having to physically visit them. In all cases this will be done with the agreement of the customer.

3.14.13.6 Self Help

Staff are encouraged to browse the Service Desk's web resources in order to discover the answers to the majority of common IT issues.

3.14.13.7 Incident Management

The primary goal of the Incident Management process is to restore normal service as quickly as possible, to minimize the adverse impact on county business. Incidents are defined as an unplanned interruption to an IT Service or a reduction in the quality of an IT Service. Incidents are given a priority to help ICT plan and allocate work, especially in busy periods. Each priority has target times. Each priority has target times relating to response (i.e. confirmation to the customer that action is being taken) and resolution.

3.14.13.8 Priority Allocation

The priority given to an incident is determined by a combination of its impact (on County, Department or individual), and urgency.

Criticality	cases	Grade	Response time
Urgent	Infrastructure failure Loss of critical systems Critical applications failure	A	
High	Service failure affecting one or more individuals	B	
Medium	Non critical systems failure Non-critical application failure	C	
standard	Request for information Peripherals failure	D	
Low	Simple requests	E	

3.14.13.9 Complaints Procedure

If there is still an outstanding issue about the service after discussion with the Support Team Manager, then the user should contact the ICT Assistant Director who will discuss the concern with the user and if appropriate, contact the ICT Director in order to agree the appropriate action.

3.14.13.10 Service Request (Task) Management

In addition to incidents, customers contact the Service Desk with requests for work such as setting up a new user, installing a new PC, or making a network point live.
Requests are of the following types and often require appointments to be made with customers:
Standard requests with defined lead times for completion Other requests will be assigned an owner within one week, and if it is agreed to go ahead, ICT will agree with the user an estimated time for completion and a charge if applicable. Occasionally a request will be significant enough to become managed as a project following the standard ICT Project Management Procedures.

3.14.14 Request Services Lead Time

The following lead times apply to normal requests regularly made through the ICT service Desk. All other requests will be assigned a user

Activity	Lead time	Description
Basic computer set up	60 minutes	Installing os, and key applications
New user set up for Applications	20 minutes	Creating accounts for systems etc.
Install wireless network	10 minutes	

point		
Phone/tablet configuration	15 minutes	Configuring email and other settings
New telephone extension	30 minutes	Installing telephone hardware in an office
Minor repairs	30 minutes	Hardware repairs not requiring part replacement
Major repairs	1 week	Repairs that require part replacement

3.15 Virtualization policy

Document: Policy	Document No.: KCG IT-015	Revision: 1.00	Effective: [Signed Effective Date]

3.15.1 Purpose

The purpose of this policy is to guide KCG ICT staff in the appropriate manner of simulation of software and/or hardware upon which other software runs. The Virtual Machine (VM) is the simulated environment which basically cuts down on costs and maximizes inter-operability and functionality of the resources. For the operational efficiency KCG can use the existing hardware (and new hardware purchases) more efficiently by putting more load on each computer.

This policy also provides a checklist of recommendations when considering engaging in use of such virtualization softwares; however it is strongly recommended that ICT staff seek expert advice when using these software.

3.15.2 Scope

This policy encompasses all KCG virtualized systems, data or information resources therein that are owned, operated, maintained and controlled by KCG and all other system resources both internally and externally that interact with these systems.

3.15.2.1 Definitions

- Virtualization - The simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM).
- Virtual Machine – It is a self contained computing resource with its own operating system and other necessary resources. It functions independently – logically speaking from the virtual machine monitor yet requires its underlying resources to work.
- Guest operating system – The Operating System which has instances where its applications runs on a separate Virtual Machine.
- Full virtualization - One or more Operating Systems and the applications they contain are run on top of the virtual hardware. Each instance of an Operating System and its applications runs in a separate VM (*guest operating system)*.
- Hypervisor – Also known as a virtual machine monitor (VMM), is a computer software, firmware or hardware that creates and runs virtual machines. It

controls the flow of instructions between the guest OSs and the physical hardware, such as CPU, disk storage, memory, and network interface cards.

- Host machine - A computer on which a hypervisor is running one or more virtual machines
- Guest machine – The virtual machines created in a host machine.

3.15.3 Policy Statements

KCG is to ensure that the virtualization policy adheres to the following conditions for purposes of complying with the mandated organizational requirements set forth and approved by ICT Management.

3.15.3.1 Data and information classification

Data and information being stored, processed and/or transmitted on system resources that are owned, operated, maintained and controlled by KCG are to have appropriate classification levels in place that consists of the following:

- Unclassified/public information
- Proprietary
- Confidential
- Company confidential
- Client confidential
- Sensitive.

An appropriate data and information classification level is to be identified and assigned for the specified system resource and documented accordingly during initial provisioning stages.
Additionally, effective data and information management measures also require KCG to define: Access rights, Usage rights (copying/printing/sending/sharing), physical security, Environmental security, network security, secure transmission, backups).

3.15.3.2 Security categorization

All system resources owed, operated, maintained and controlled by KCG are to have in place effective measures for ensuring their confidentiality, integrity, and availability. The categories are: LOW, MODERATE, HIGH and CATASTROPHIC.

3.15.3.3 Personnel

Authorized personnel in KCG are deemed the employees responsible for general provisioning, maintenance and security of virtualized systems. Enhancing of applicable skill -sets and subject matter knowledge of the personnel which are relating to the virtualized systems.

3.15.3.4 Physical Security

Appropriate security measures are to be implemented, which includes all necessary physical security controls, such as those related to the safety and security of the actual hardware(i.e. servers) for which the virtualization software system reside on. This requires the use of a computer room or other designated area (facility) that is secured

and monitored at all times and whereby only authorized personnel have physical to the specified system resource. Thus, "secured" and "monitored" implies that the facility has in place the physical security and environmental security controls.

3.15.3.5 Security Awareness Training

All employees within KCG are to undergo annual security awareness training initiatives for they stay abreast of significant security issues that pose a credible threat to KCG as a whole, including, but not limited to, KCG's network infrastructure all supporting system resources. While the goal of the program is to have in place a comprehensive framework that effectively addresses the core components of *Awareness, Training* and *Education* the program must also provide subject matter directly related to the security of Virtualized systems.

3.15.3.6 Provisioning and hardening

All systems, specifically the host O/S and other supporting hardware and software utilities, are to be properly provisioned, hardened, secured, and locked-down for ensuring their confidentiality, integrity and availability. Improperly or poorly provisioned systems can often result in network exploitation by hackers, malicious individuals, and numerous other external, and internal threats. Therefore, the following provisioning and hardening procedures are to be applied as necessary when deploying the virtualized environment.

i. Virtualized systems onto KCG network
ii. Vendor-supplied default settings are changed.
iii. All unnecessary accounts are eliminated.
iv. Only necessary and secure services, protocols and other essential services are enabled as needed for functionality.
v. All unnecessary functionality is effectively removed.
vi. All system security parameters are appropriately configured.
vii. Documented system configuration standards.

4.0 THE STANDARDS

4.1 Acceptable use of ICT facilities in the public service

4.1.1 General Directives

KCG information resources, all types of application software, hardware, network facilities, and similar devices, must be used appropriately, responsibly and with accountability. Any damage to ICT properties or corruption of software and data as a result of the user's negligence shall be dealt with accordingly upon validation of fault. When using KCG ICT resources the following requirements must be adhered to:

- All concerned shall take appropriate action with due diligence to comply with hardware warranty or conditions of use, software license agreements and respect of the rights of other authorized users of the facility.
- Users shall be accountable for their ICT facility personal access accounts and the personal access accounts of others. Each user is obliged to report unauthorized access or transactions.

- Each user is accountable for his/her own work or data, and accountable for the work or data of other users of the ICT facility.
- Users shall use only the machines or component ICT facilities for which they are authorized.
- Access accounts must be used for intended purposes only. KCGICT facility shall be used for purposes of KCG related work only.
- All users must cooperate with the systems administrator. The systems administrator is authorized and may access the user's work or data if deemed necessary to maintain a secure environment and ensure effective and efficient use of the ICT facility.
- All users are directed to report any illegal activity and wrong-doing to Responsible Business Unit Managers and ICT department in KCG ICT Common Services. In the event of an official investigation, all users are mandated to cooperate to the fullest extent of their capacity and authorization. The ICT department in KCG shall ensure proper communication and documentation of County Government expectations for handling sensitive data.

4.1.2 Use of ICT Hardware and Software Resources

4.1.2.1 Hardware Management

Any installation or deployment, configuration and maintenance of computer equipment are the responsibility of the ICT department. Maintenance action or procedures shall comply with enforced warranty or related maintenance agreements.

4.1.2.2 Hardware Documentation

The ICT department shall maintain a register (inventory) of the County Government's ICT equipment. This includes custodian list, Local and Wide Area Network setup/diagram, systems specifications, and configurations. A periodic inspection and update of register shall be conducted by the ICT department. The inventory shall include IT special projects or any IT related undertaking of the KCG.

4.1.2.3 Hardware Protection and Insurance

The ICT Department will liaise with concerned office to ensure adequate insurance coverage for ICT equipment/facility. Likewise, ICT department shall ensure that adequate facilities which are critical to the physical protection of the device or its environment are installed to prevent or minimize the effect of fire, flooding, and similar physical threat. The ICT Department will ensure that staff are aware of restrictions and limitations.

4.1.2.4 Procurement

Procurement of ICT equipment in amounts in excess of Kshs 10 million is subject to the approval of the ICT Strategic Plan Steering Committee. Any ICT procurement valued at less than Kshs 10 million, approved by Senior Management, shall require review of the ICT department. Requirements for new hardware and software should be discussed in advance with the department to assess the detailed specification of the equipment.

And a written technical advice from the ICT department to the procuring entity shall be part of the presentations to the ICT Strategic Plan Steering Committee.

4.1.2.5 Movement of ICT Equipment

Any movement of ICT equipment or transfer of custody shall be duly coordinated with the ICT department for necessary processing (update of register and insurance policy). Movement or transfer shall comply with requirements on disposal, servicing, transfer of ICT equipment. Movement or transfer shall not be left to any individual, or private sector organization or person.

4.1.2.6 Use of Portable Equipment

Laptops, multi-media display, or any portable media, or other ICT equipment used outside of the KCG premises for official business shall be logged in/out for proper tracking of equipment movement. The security and safekeeping of portable and other equipment used outside of Government premises is the responsibility of the staff using it.

4.1.2.7 Designation or Sharing of Portable Equipment

Distribution or assignment of laptops or notebook PC or any similar portable computing device should follow "Function vs. Equipment Assessment" result as presented in the Operational and Strategic Planning section of this standard. Designation of a portable computing device to a specific employee position shall follow the general rules on care and manufacturer instructions. Portable computing devices designated to be common (shared) shall be managed solely by the ICT department.

Portable Device Request Procedure:

- Fill out form for request.
- Submit to ICT department for immediate processing
- The ICT department facilitates availability of unit upon approval
- The ICT department releases the unit to the requesting party

Note: The requesting party should not be the one to get the device from previous user.

4.1.2.8 Software Installation

The ICT department is responsible for all software installation, deployment and configuration on all KCG-owned ICT equipment. Unauthorized software installed will be deleted without need to notify the user.

4.1.2.9 Loss or Damage to ICT Equipment

In the event of loss or damage to any ICT equipment the rules and regulations, as outlined later, will be followed.

4.1.2.10 Portable Storage Devices

KCG provided portable external storage devices should be given appropriate care by the employee in custody as described in the manufacturer's instruction for care.

Any personal portable external storage device upon processing (registration, scanning, sanitizing, etc.) of the ICT department and approved for use within the KCG's ICT Facility shall be the responsibility of the owner of the device.

Loss or damage of said device or data stored therein shall be the responsibility of the owner or any loss or damage caused by the device to any KCG owned ICT equipment shall be the liability of the owner of the personal device.

4.1.2.10 Schedule of User Performed Hardware System Maintenance

It is mandatory for all employees with designated PC system or with personal computing/storage device to schedule and perform the following maintenance at least once per week, as appropriate:

- scan and clean systems from computer viruses (full scan)
- clean the registry
- check hard disks for errors
- defragment the hard drive

4.1.2.11 ICT Equipment Care

All employees shall be responsible for the proper usage, care and cleanliness of the ICT equipment they use. Responsible Business Unit Managers shall ensure that their staff maintains the cleanliness of their machines. Only approved and authorized cleaning solutions and materials shall be allowed for use.

4.1.2.13 Safety Precautions

Health and safety with regard to use of computer equipment and computer workstations should be managed within the context of the general and specific Health & Safety policies and procedures of KCG.

4.1.2.14 Cables, Links, Wire etc.

Only power cables and accessories and the like that come with ICT equipment and portable devices like multimedia projectors, should be used. Any alternate use of cables, links, wire, etc. shall require authorization from the ICT department.

4.1.2.15 Non Government Users

Visitors, guests or even government employees from other agencies are prohibited from using any ICT facility owned by the KCG unless given explicit permission by the supervisor or senior officer of the unit, section or office visited.

4.1.2.16 Service Requirements

Problems with hardware should be reported to the ICT department and ICT officer within department. Servicing of any ICT equipment should not contravene with any related agreement, laws on Intellectual Property, license agreement etc. Outsourced servicing of ICT equipment should conform to this standard document.

4.1.2.17 Software

All employees are instructed to protect software license agreements as defined in the software licenses' section in this document.

4.1.2.18 Miscellaneous Devices and Accessories

All ICT devices and accessories attached to any ICT equipment, systems or network such as PC Desktop Camera, Wireless USB modem, Scanners, etc. shall be given appropriate care. Loss or damage due to misuse or intentional cause is considered a grave offense.

4.1.3. Security

4.1.3.1 New Appointments

Responsible Business Unit Managers should notify the ICT department to allow the creation or deletion of network and e- mail accounts and PC system permissions for new staff and for staff leaving the unit.

4.1.3.2 User responsibility

Users should change their access codes when prompted by the system in the case of networked machines or on a regular basis for standalone machines.

4.1.3.3 Protection against viruses

Viruses or such worms are detrimental to performance of an electronic system, and they must be prevented and eradicated.
Users, whether standalone or networked, should clean viruses on their computers on daily basis.
The ICT department shall ensure that KCG has antivirus software with which users can ensure that their systems are virus free.
The ICT department shall configure antivirus on the KCG Wide Area Network servers and clients such that cleaning of viruses on the network is automatic.
MDAs shall ensure that they have a standalone computer on which removable data storage mediums can be cleaned off viruses before use of the removable data storage mediums into other computers. Otherwise, use of removable data storage mediums from one computer to another is prohibited.

The ICT department will provide facility, assistance and training when required.

4.1.4. Use of e-Mail

4.1.4.1 General Directives on Use of KCG provided e-Mail System:

Electronic mail or "e-mail" systems are important alternative means of communication. In certain business functions, e-mail is preferred more than other conventional methods of communications. When using the KCG e-mail system the following general considerations apply:

- Minimize Messages - For KCG provided e-mail accounts, employees should minimize the number of messages in their e-mail in-box to ensure efficient function of the e-mail system.
- Maintenance of Messages - Garbage messages should be deleted regularly. Folders should be set up and messages filed accordingly.
- Archiving and storing - Employees should utilize the archiving facility within the e-mail system in accordance with allowed storage capacity and guidelines.

- Accounts and passwords - A register of e-mail accounts and passwords updated regularly shall be maintained by ICT department.
- Password and account expiration - It is mandatory to change e-mail passwords every 30 days or as necessary. The e-mail accounts of employees separated from the KCG shall be processed and deleted upon approval of Senior Management.
- Password security – Users should safeguard their electronic identity. Sharing of password, for example, is prohibited.

4.1.4.2 Examination of e-Mail Use

KCG retains the right to access and view all e-mails sent and received by the KCG e-mail system. All employees whether regular, contractual, or circumstantial are required to give consent to the examination of the use and content of their e-mail accounts with due approval of Responsible Business Unit Managers and in strict observance of personal privacy. This right is exercised solely through the ICT department upon official written instruction of a member of Senior Management.

4.1.4.3 Limitations on Personal Use

Very limited use of KCG provided e-mail system for personal use is permitted. However, Responsible Business Unit Managers should ensure that there is no abuse of this privilege. Personal use of KCG e-Mail account may only occur under the following circumstances:

- Use and access only during work breaks or after office hours,
- Personal use of e-mail should not interfere with work.
- Personal e-mails must adhere to the guidelines in this standard.
- Personal e-mails must be kept in a separate folder, named 'Private'. The e- mails in this folder must be deleted weekly so as not to clog up the system.
- The forwarding of chain letters, junk mail, jokes and executable files is strictly prohibited.
- Mass mailing is strictly prohibited.
- All messages distributed via the KCG e-mail system, even personal e- mails, are KCG property.

4.1.4.4 Group Sending of e-mail

Group/List sending of e-mails should be used appropriately. Spamming is prohibited. E-mail to all staff (broadcast) concerning official business function should be used only when appropriate.

4.1.4.5 Confidential Materials

Official and confidential materials sent through e-mail should be encrypted. The ICT department will provide encryption tools.

4.1.4.6 Non-Government e-mail Systems

For Civil/commercial provided e-mail systems, employees should seek approval from Senior Management, through ICT department before accessing or using any said accounts on any KCG provided ICT equipment. At a minimum, only the following conditions shall be the basis for approval:

- If the Civil/commercial account will be used for official business function only.
- If the employee seeking approval, as a condition, shall permit the KCG to access and review the account as required.

4.1.4.7 E-mail Access Using KCG ICT Resources

KCG IT resources used to operate KCG provided e-mail service or Civil/commercial operated e-mail services must not be used for the following:

- Political, commercial and personal purposes not related to the Government.
- Illegal, pornographic, or cause to harm any entity, or any inappropriate material.
- Sending or forwarding e-mails containing libelous, defamatory, offensive, racist or obscene remarks, or any similar nature.
- Forwarding messages without acquiring permission from the sender.
- Sending/Forwarding unsolicited e-mail messages.
- Forging or attempting to forge e-mail messages.
- Sending e-mail messages using another person's e-mail account without permission from the originator.
- Copying messages or attachments belonging to another user without permission from the originator.
- Disguising or attempting to disguise one's identity when sending e-mail.

  Note: If you receive an e-mail of this nature, you must promptly notify the network administrator.

4.1.4.8 Signature

A Signature must be included on all emails that include your name, job title and agency name. A disclaimer will be added underneath your signature (see Disclaimer)

4.1.4.9 Disclaimer

The following disclaimer will be added to each outgoing e-mail:

'This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this e-mail in error please notify the system manager. Please note that views or opinions presented in this e-mail are solely those of the author and do not necessarily represent those of the Kisii County Government. Finally, the recipient should check this e-mail and any attachments for the presence of viruses. The Kisii County Government accepts no liability for any damage caused by any virus transmitted by this e-mail.'

4.1.5. Internet Use

4.1.5.1 Purpose of Use

Access to the Internet is provided for official purposes; therefore, any act relative to the use of KCG provided internet access should be for official purpose only.

4.1.5.2 Examination or Monitoring of Internet Use

KCG retains the right to monitor the Internet usage of employees. All employees, whether regular, contractual, or circumstantial, shall give consent to the examination of the use and content of their internet activity/history as required, with due approval of

Responsible Business Unit Managers and in strict observance of personal privacy. This right is exercised solely through ICT department and, where relating to a specific staff, only on written instruction from an authorized official and related to a legitimate government function.

4.1.5.3 Limitation on Website Browsing

Access or any act similar to viewing pornographic, obscene, violent, gambling, illegal or other similar web sites using Government provided internet facility is prohibited. KCG employees are duty-bound to report such abuse by co-employees. This standard also applies to access using non-Government provided internet but within the premises of the KCG and using or not using any KCG provided ICT resources.

4.1.5.4 On-line Communities, Subscriptions and other Web 2.0 Services

It is prohibited to operate, participate in, contribute to on-line communities or subscribe to other similar on-line groups over the internet while in the workplace unless permission is officially granted by Senior Management. Below are conditions for approving permission:

- On-line Communities/Subscription is to support or improve work related tasks
- On-line Communities/Subscription sites operate in secure environment and this should be verified by ICT department.
- On-line Communities/Subscription does not entail cost to KCG
- Participation in On-line Communities/Subscription does not violate KCG ICT policy, rules and regulations and any local and national law.

4.1.5.5 Programs and Executable Files

Any program or executable file, including screensavers, or any similar format when using KCG provided machine through KCG provided internet access are not to be downloaded. Any required program or application required in performance of an official function shall be sourced through the ICT department. This is to prevent indiscriminate downloading and installation of programs or applications that may slow down ICT resources performance and at worst, threaten security of facility.

4.1.5.6 File Download

Downloading of movies, video, music, images and similar file formats not related to any official or legitimate KCG function is strictly prohibited. Scanning for virus is a mandatory pre-requisite before opening any file or program downloaded through the internet.

4.1.5.7 Secure Internet Access

All employees who have access to the internet should ensure the use of said facility does not compromise stability and security of the ICT facility environment. Should anyone accidentally/mistakenly allow this to happen, the systems administrator must be notified immediately.

4.1.6. Network Use

4.1.6.1 General Network Access

Network facility and bandwidth is limited, therefore access and use of the facility is managed according to priorities and importance. Below are limitations to the use;

- Access shall be on a 'work process reserved' basis.
- The ICT department does not guarantee Internet connection reliability and consistency, only the reliability of the WAN (The ICT department controls the WAN, but Internet service is provided by external ISPs).

4.1.6.2 Network Management:

Network installation, administration and maintenance within the KCG are the responsibility of qualified and authorized ICT department Staff only. Access to, and management of the Network Servers are restricted to authorized staff.

4.1.6.3 Network Access Information

Disclosing any assigned IP address, Systems Administration password and any similar key that may compromise access, security of network and data is prohibited. Any knowledge of such disclosure should be reported to ICT department.

4.1.6.4 Tampering and Unauthorized Access

Unauthorized connection physical or virtual to any framework or device; or tampering of network cables or any similar device within the KCG is prohibited and will constitute grave offense. Any knowledge of such activity should be reported to ICT department.

4.1.6.5 Jeopardizing Network Integrity

Any action that may damage, destroy, and negatively affect performance or any similar act that may intentionally or unintentionally jeopardize any network device or facility is prohibited. Any cost incurred out of such recklessness or negligence shall be borne by the person liable.

4.1.7. Use of Wireless Communications

4.1.7.1 Unauthorized Installation of Wireless Hardware

Connecting or attempting to connect a wireless device to the KCG Internet or LAN wireless service is prohibited unless approved by ICT department.

4.1.8. Miscellaneous Provisions for Internet Use, E-mail and Other ICT Resources

4.1.8.1 Unacceptable Personal Use

Described herein are general acts considered to be unacceptable use of ICT resources. These may be acts to interrupt official business operation, cause undue loss, damage or cost to the KCG, and embarrassment.

- Violation of Law. Act to violate, encourage violating, accomplice to a violation of the KCG's rules and regulations and any local or national law.

- Illegal Copying. Any act of copying or any act of similar nature using copyrighted materials of any format as prohibited by copyright or intellectual property regulations.
- Operating a Business. Directly or indirectly using the KCG's facility to operate any non-Government related business is prohibited.
- Gaming, Gambling or Wagering. Accessing, operating or simply viewing any gambling activity over any Government-owned ICT facility is prohibited. This extends to computer gaming and any form of entertainment not related to official business function.
- Solicitation. Except for KCG-approved programs, soliciting for money or support on behalf of charities, religious entities or political causes is strictly prohibited.
- Political or Partisan Activities. The use of any ICT facility to promote, advocate, distribute any material, or any act of similar nature, for political or partisan politics is prohibited.
- Compromise Integrity of the ICT Facility. Any act that will reduce the reliability, compromise fidelity, or any action of similar nature that will negatively affect the integrity of the ICT facility is prohibited.
- Acts that Waste ICT Resources. Any act that depletes, expends or any action of similar nature that wastes resources including but not limited to, excessive printing of documents, storing unnecessary files on hard disk drives, storing unimportant e-mails on KCG provided e-mail systems, transmission/ extraction of large files over the network or internet, etc. is prohibited.
- Web 2.0 Use. Web 2.0 technologies include on-line communities, on-line forums, chat rooms, instant messaging, blogs, wikis, webo's, peer-to-peer file sharing, and social networks. Employees must obtain permission from their department supervisor and ICT department to use any of these technologies in the workplace. Any employee permitted to participate in any of the above means of communication should comply with the rules and regulations of the KCG, the KCG's ICT policy and any related local and national law.
- Obstruction to ICT Resources. Impede, directly or indirectly cause a delay, encrypt or conceal, or do any similar act that will limit or prohibit the KCG from accessing, operating, monitoring, and reviewing ICT resources is prohibited. Only authorized ICT department staff shall be allowed to set or manipulate passwords on any KCG-owned common ICT resources, and/or limit the use of ICT resources by specific employees with the approval of Senior Management.
- Falsification or Misrepresentation. Falsifying any electronic document or misrepresenting one's identity or association to carry out an unauthorized, unlawful, offensive act through electronic communication whether using KCG-owned ICT resources or personal devices within the premises of the KCG is strongly prohibited.
- Restrictions on the Use of KCG provided E-mail Addresses.
  KCG employees shall avoid use of KCG provided e-mail addresses such as firstname.surname@kisii.go.ke for personal communications in civil forums or sites of similar nature unless approved by Senior Management, for official purposes only. This is to avoid any personal opinion being interpreted as a KCG opinion.

- Violations of Civil or Private Systems Security Measures. Any use of KCG provided ICT resources to manipulate or compromise the security or operation of any Civil or private computer systems is prohibited.
- Violating Data Privacy or Confidentiality Procedures. Using KCG provided ICT resources or personal device inside or outside the KCG premises to violate or attempt to circumvent data or confidentiality procedures is prohibited.
- Accessing or Disseminating Private or Confidential Information. Accessing or disseminating private or confidential information about another person whether the person is an employee or non-employee of the KCG, using KCG-owned ICT resources without proper authorization is prohibited. Prohibition includes falsifying of such information.
- Accessing Systems without Authorization. Accessing files, systems, networks, account of another person and similar devices within the KCG provided ICT resources are prohibited. Each employee is accountable for the safeguarding of their PIN, passwords or keys in accordance to related policies.
- Distributing Malicious Code. Distributing malicious code or similar format such as computer virus, spyware, malware is prohibited. Prohibition includes intentional keeping of malicious codes.

4.1.8.2 No Anticipation of Privacy

In general, no employee should expect or demand privacy in using KCG provided ICT resources. At any time, with the approval of Senior Management, and for official purpose, ICT department may subject the ICT resource to review, inspection and investigation.

4.1.8.3 User Agreement to the Terms and Conditions of this standard:

Relative to the use of the KCG ICT Equipment, KCG Network Facility, KCG e-mail systems, or any of the KCG related ICT components and parts, the user shall agree to the terms and conditions of this standard. All employees will be required to sign an ***Acknowledgement of Receipt and Understanding Form***, attached as Annex 8 to this standard, to certify their willingness to comply with the acceptable use provisions.

4.1.9. Disciplinary Action

The violation of the provisions of this standard will lead to disciplinary action. Penalties provided will be based on the Disciplinary Procedures set out in the pertinent civil service laws.

4.2. Electronic records management

4.2.1. Definitions

The *ICT Glossary and Definitions* contains a description of any common ICT terminology referred to in the policy and standard documentation.
For the purposes of this *ICT Standard and Guide for Electronic Records and Document Management* and all associated and related documentation and processes, the terms ‘ document ’ and ‘documentation’ include any recorded information or material, in electronic format, which conveys coherent information for human understanding and use.

The terms 'document' and 'documentation' also include any recorded information, including, but not limited to, textual data, graphical, visual, audio and electronic information.

4.2.2. Standard and Regulations

The *ICT Standard and Guide for Electronic Records and Document Management* applies specifically to appropriately authorized and approved documentation that is stored electronically, transmitted on the WAN, or hosted on KCG Websites.

These document hierarchies provide repositories for electronic documentation of interest to the KCG and individual teams within Ministries/Departments. The level of accessibility granted to a specific document will be determined prior to the approval and release of that document.
ICT staff will have access to other network file storage and a range of local file storage. This document does not apply to these areas.

4.2.2.1 Regulations

- Policies and documents for inclusion in the KCG Calendar shall be reviewed by the ICT director. Once reviewed, these documents maybe tabled and approved by various governance committees of which ICT staff are members. Once approved, they will be sent to the person responsible for amendments to the KCG Calendar for inclusion in the next update.
- All other ICT documents stored in the KCG Website, shall be approved by an appropriate ICT staff member or committee, commensurate with the level of risk, confidentiality, audience and significance of the document and issues discussed in the document.
- All documents shall be published in PDF format to preserve their integrity. The original source documents will be stored in a secure format.
- All documents that improve the level of assurance, business continuity, and delivery of the range of products and services provided by ICT shall be stored electronically.
- Each document shall contain a Document Information and Version Control statement on the first page of the document.
- All printed documents shall be treated as Uncontrolled. The Controlled version shall be the electronic version.

4.2.2.2 Objective–ICT Document Management Process

All documentation subject to this standard should adhere to the ICT Document Management
Process.
The ICT Document Management Process regulates and guides the lifecycle of every document created by, and for, the Government of Kisii. In brief, the process helps ensure that each document is:

- Created in a standard and reliable format, with accurate content and common naming conventions.
- Correctly maintained to ensure continued accuracy and validity.
- Accessible from designated locations (electronic).

- Securely archived (and eventually destroyed) when the document no longer services an existing process.

4.2.2.3 Process Overview- ICT Document Management Process

The Document Management Process regulates the entire lifecycle of every document created within that process, and is comprised of the following six sub- processes:

1. Creation
2. Approval
3. Publication
4. Maintenance
5. Archive
6. Destruction

An original source copy of every published document shall be stored in the Documentation Framework site.

This site will be used as the primary storage and workspace/collaboration area for all ICT policies, standards and guidelines. Documents shall be created, edited and maintained in this site. Once a document is ready for release, a copy shall be converted to Adobe Acrobat (PDF) format and published to the relevant location.
All URL references within a document shall be linked to the published version of the reference. An edited document when released for publication shall overwrite the existing published version, to ensure that links to the document remain valid.

4.2.2.4 Documentation Register

For each document stored electronically, the following details shall be provided:

- Location where published
- Document Title
- Date Published
- Who Published
- Review Date.

Documents will be reviewed at least annually.

4.2.3. Document Management Guidelines

These guidelines outline the various management stages of a document lifecycle from creation, approval, publication, maintenance, archive, and ultimately destruction of a document in line with the Document Management Process of the Government of Kisii.

4.2.3.1 Publishing Process Overview

The publishing process shall ensure that approved documents contain accurate and up-to-date creation, approval, and maintenance information, and that only the most recent version of any document is available for access and use.

4.2.3.2 Maintenance Process Overview

All documents shall be allocated a review period of not more than one year. In addition, all staff are required to notify an Owner where an inaccuracy or problem is

identified in an approved document, and Owners must then initiate an update of the document.

The document's Review Date is typically set at 12 months from the date the document was last reviewed. Where it is believed that a document will require review within the 12 month period, a shorter period (i.e. closer Review Date) may be set, at the Owner's discretion. In any case, documents may not be allocated a Review Date exceeding 12 months from the date the document was last reviewed.

4.2.3.3 Archive Process Overview

The majority of documents stored in the Documentation Framework Site relate to the provisioning of current services, systems, and processes. In many instances, the implementation of new versions negates the need to retain superseded version documentation.
CD and DVD copies shall be retained for a period of 7 years and then will be removed from the archive and destroyed.

4.2.3.4 Destruction Process Overview

If a document does not require archiving, it shall be destroyed either when a new version is created or updated, or when the Owner advises that the document is no longer required. Archival copies of documents will be destroyed after a period of 7 years has elapsed from the creation of the CD or DVD archive version.

4.2.3.5 Roles of various officers in Document Management

4.2.3.5.1 Senior Manager

The Senior Manager in this case is the manager of each section responsible for the process. In such cases where the Senior Manager is not available, the next person in charge can perform the tasks as required.
Note: Where a Senior Manager is also the Author and Owner of a document, another staff member must perform the Senior Manager's reviewing responsibilities.
Senior Managers shall:-

- Approve release of the document for publication after the owner has released the document for use.
- Ensure the document does not duplicate the content or purpose of an existing document.
- Ensure the document uses the correct template and file naming conventions.
- If the Owner of a document has left the section, Senior Managers must allocate any of the Owner's documents to a new Owner. In such cases, until a new Owner is allocated, the Senior Manager becomes temporary Owner of those documents.

4.2.3.5.2 ICT Director

In such cases where the ICT Director is not available, a Senior Manager, or other delegated representative of the ICT Director, can perform the task as required.

Note: Where the ICT Director is also the Author and Owner of a document, another staff member must perform the ICT Director's reviewing responsibilities.

The ICT Director shall:-

- Schedules periodic audits of the content and quality of the Document Management Process.
- Approves modifications to the ICT Document Management Process.
- When new or amended policies, standards, or guidelines are introduced, the ICT Director assesses the implications of these new policies, standards, or guidelines, and initiates the creation of new policies, standards, and guidelines, or the amendment of existing policies, standards, and guidelines, as necessary.
- If a Senior Manager, being the Owner of a document, has left the section, the ICT Director must allocate any of the Senior Manager's documents to a new Owner. In such cases, until a new Owner is allocated, the ICT Director becomes temporary Owner of those documents.

4.2.3.5.3 ICT Staff

KCG staff is not only the end users of documentation, they also play an integral part in ensuring that document management works.

ICT staff shall ensure that:-

- They do not store obsolete documentation.
- They do not make unauthorized copies of documentation, including printed copies, electronic copies, or storage of electronic copies in unauthorized locations.
- Any undocumented process is brought to the attention of their Senior Manager, and that a document creation is initiated.
- Any modifications to a process affecting its documentation are brought to the attention of the document Owner to ensure modifications occur within one week.
- Any unauthorized documentation used by ICT staff is re-created and processed through the Document Management Process.

4.2.4. Document Management Standards

These standards outline the various syntax and regulations that will apply to the conventions applied as part of a document, in-line with Document Management Process within the Government of Kisii.

4.2.4.1 Document Title

With the exception of forms, templates, and spreadsheets, the document title appears:

- In the body of the document's cover page
- In the header of the document's cover page
- In the header of the document's body content

As part of the document's electronic file name the following exceptions apply:-

Forms:

The document title appears as part of the document's electronic filename, which is located in either the header or the footer of the document, as appropriate.

Spreadsheets:

The document title appears as part of the document's electronic filename, and is displayed in the title bar of the spreadsheet application.

Templates:

The document title appears as part of the document's electronic filename. The document title does not otherwise appear in the document.

4.2.4.2 Rules

- Document titles must accurately and concisely represent the document's
  Purpose.
- Where a document will have the same name and/or purpose for more than one department/agency, the document title must include the name/acronym/initials of that section.

4.2.4.3 Version Numbering

Version numbers shall be allocated by the Owner. Every document will have an identifying version number. With the exception of forms, templates, and spreadsheets, the version number must be displayed in the Document Information table located on the document's first page

4.2.4.3.1 Version Number Formatting

Version numbering is broken down into two types:
1. Draft version numbering
2. Active Change version numbering

Draft version numbering is displayed in the following format: V*n.n*
Where: V: is always presented in uppercase
N: is a number from 0 to 9.
Active Change version numbering is displayed in the following format: V*n.n*
Where: V: is always presented in uppercase
n: is a number from 0 to 9.

4.2.4.3.2 Draft Version Numbering

A document is considered to be in Draft stage from the time it is created until it is approved. During creation, the document shall undergo continual review and modification until it is approved.
Draft version numbers shall appear to the right of the decimal point in the version number (the zero on the left side of the decimal point never changes in a Draft document version number). The Draft version number increases by one minor version with each review and modification. For example:

Modification	Version Number (increases)
First draft	V0.1

Second draft	V0.2
Third draft	V0.3

Where a document has gone through more than 9 drafts (i.e.V0.9), the version number format may be extended to V0.*nn* (e.g. V0.11).

4.2.4.3.3 Active Change Version Numbering

Active Changes only occur to approved documents. An Active Change is any change made after a document has been approved.
When a Draft document is approved, its version number shall change to V1.0. This is the first 'live' version of the document, and means it is approved for use. Any further changes to the document cause the version number to increase by one minor version from V*n*.1 to V*n*.9, and then increase by version in sequential order. For example:

Modification	Version Number (increases)
First change	V1.1 (was V1.0- increases by.1)
Second change	V1.2
Third change	V1.3
…	

Tenth change	V1.10
Eleventh change	V1.11
Twelfth change	V1.12

After a document has been reviewed, the version number shall change by 1 increment (e.g. review done after twelfth change, V1.12 changes to V2.0).

4.2.4.4 Related Documents Information

For Policies, Standards, Guidelines, Minutes and other documents as required, the Related Documents section of each document includes a list of documents related to the contents of that document. If these documents are stored electronically, a link should also be part of the document name.

4.2.4.4.1 Related Documents Categories

Related documents are divided into four categories:

1. Policies, standards and guides
2. Procedures
3. Forms and templates
4. Other

For each document listed in the Related Documents section, the following information is required:

- Document (Electronic): The Document file name: (e.g. Document Standards and Conventions).
- Note that neither the version number (e.g.V1.0) nor the file extension (e.g. .doc) should be included.
- Location (URL) of the published version of the document.

4.3. Information Asset Classification and Control

4.3.1. Definitions

"Information Assurance" is concerned with the protection of information and information systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation of information operations.
It includes providing for restoration of information systems by the incorporation of appropriate protection, detection and reaction capabilities.

This Information Asset Classification and Control Standard requires agencies to implement policies and procedures for the classification and protective control of information assets (in electronic and paper-based formats) which are commensurate with their value, importance and sensitivity.
All physical information assets (including hardware and software) used to process, store or transmit information must be accounted for. In addition to asset inventories, all major information assets used in an organization's operations must be identified and an owner assigned for the maintenance of appropriate security controls.

4.3.2. Standards

1) Inventories of all major information and ICT assets should be maintained;
2) Information will be classified according to its sensitivity and importance, taking into account the organization's requirements for the sharing or restriction of information, legal and/or legislative requirements and probable impact resulting from unauthorized access or damage to the information. To achieve and maintain appropriate protection of the organizational information assets:-
   - All assets shall be clearly identified and an inventory of all important assets drawn up and maintained;
   - The organization will adopt the Business Classification Scheme for the purposes of classification of "public records" and disposal schedules;
   - All information and assets associated with information processing facilities shall be "owned" by a designated part of the organization. The owner shall be an organization's Senior Manager/System Sponsor or the ICT department and

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

3) KCG's information classification scheme will be based on the following qualifications:-
   - Information will be classified as either Public or Non-Public;
   - Non-Public Information will be classified as either Unclassified or Classified;
   - Classified Information will be classified as either Secure or Sensitive.
4) Confidentiality, integrity and availability of sensitive or secure information will be appropriately protected throughout the information lifecycle: collection; storage; use; transmission; disposal.
5) If information is stored in the Data Centre, the security classification will be Commensurate with the zone where the information is located.
6) The department's Senior Manager or the ICT Director ("Officer") is responsible for ensuring an information technology resource and/or the information contained within, is classified as: Public; Sensitive;
7) Or Secure Information. Security measures will be implemented according to the information classification.
8) Sensitive or secure information will be appropriately protected independent of location and technology. To ensure that information receives an appropriate level of protection:-
   - Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the department.
   - An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification system adopted by the department.
9) Authority to lower an information classification must be obtained from the owner of the information source.
10) KCG employee or citizen personal information shall be classified as at least sensitive information.
11) Core Information Systems will be identified and information assurance responsibility assigned to the Core System Sponsor unless otherwise indicated.
12) KCG Staff should agree to a confidentiality agreement prior to commencement of formal duties and the agreement should be reviewed annually or whenever there is a change in terms of employment.
13) Classification schemes do not limit the provision of relevant legislative requirements under which the organization operates.
14) Disposal of public records shall be in accordance with KCG's Records Disposal Policy.
15) The archiving of information and documents shall be in accordance with the KCG's Archives Policy and Procedures.
16) Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

17) Removal off site of the organization's sensitive information assets, either Printed or held on computer storage media, should be properly authorized by management. Prior to authorization, a risk assessment based on the criticality of the information asset should be carried out. At a minimum, where information is classified as "Classified – Secure" or "Classified – Sensitive", a Confidentiality Agreement between KCG and the Organization contracted to perform services for the KCG where access to this information is required shall be signed and processed through the appropriate Legal Office.

18) Responsibility remains with KCG, therefore these obligations must be considered when entering into arrangements that permit access to sensitive and/or secure information with a third-party (e.g. Vendor support, contractors, associated organizations).

4.4. Information Systems Security Management

4.4.1. Introduction

4.4.1.1 Goal

Support the County Government of Kisii (KCG), through the ICT Department, in running one of its core functions, namely: development and implementation of information systems and technology develop and manage integrated information technology infrastructure, optimization of resource utilization and installed infrastructure.
Protecting the confidentiality, integrity, and availability of information assets from any disruption and threats both from within the KCG or from external parties, whether intentionally or otherwise.

4.4.1.2 Scope

This standard applies to all assets used to secure the management of KCG information, and is used within all departments and related units as well as providers and users of KCG public service. The scope is also defined in terms of organization and locations. This standard applies at ICT department and all units throughout KCG, relevant government agencies, business partners and other third parties.

4.4.1.3 Definition

1. Information asset in this standard is information and the processes of its gathering, processing and distribution. Information assets include:-
   a) ***Data/documents:*** Economic and financial data, payroll data, personnel data, tender documents and contracts, document management system(s).
   b) ***Software:*** Application software, system software, system development toolkit, and other assistive devices (antivirus, audit tools).
   c) ***Physical infrastructure:*** Computer equipment, networking and communications equipment, removable media (e.g. flash, CD, DVD, diskettes), and other supporting equipment (e.g. UPS, generators, communications antenna).
   d) ***Intangible assets:*** Including knowledge, experience and expertise, image and reputation.

2. Information Security Management Policy is a framework for security management of information assets using a risk based approach in formulating, implementing, executing, monitoring, reviewing, maintaining and improving information security performance.

3. Information Asset Owner is the party that is legally designated as being responsible for the information asset or work processes in the KCG or the management of agency/department units where the data or information was created or is stored.

4. Chief Information Security Officer is an official appointed by the ICT Strategy Plan Steering Committee to coordinate and direct the activities of the application of information security policies and procedures within the agency where he/she is assigned. The Chief Information Security Officer is to coordinate with similar officials in other agencies either directly or through the Information Security team to resolve existing problems.

5. Permissions are powers/rights related to the use of an asset type and level of information tailored to the needs of a specific business process, that has been granted based on related information security risks. This right, depending on the type of asset, is formally granted or authorized by the owner of the asset.

6. Risk assessment is the entire process of analysis and risk evaluation.

7. Risk Evaluation is a process that compares the estimated magnitude of a risk with already well-defined criteria to assign levels of risk.

8. Information security incidents are events that are not desirable and that violate the policy or procedures of the ISMS that poses a threat to the security of information assets or results in disruption of the work process of the organization.

9. Mobile Computing is the use of portable computing devices (portable), such as notebooks and personal digital assistants (PDA) to access, data processing and storage.

10. Tele-working is the use of telecommunications technology to enable employees to work at a remote location from the office.

4.4.1.4 References

I. ISO / IEC 27001:2005 Information Security Management System, Standard II. ISO / IEC 27002:2008 Information Security Management System, Guidelines III. ISO / IEC 27005 (BS7799-3: 2006) Risk Management System

4.4.2. Information Security Management Policy

4.4.2.1 General Policy

1. Comply with all laws and regulations applicable including the legal obligations to protect its information assets.
2. Comply with the requirements as well as operational and technical standards as contained in the overall information security policies and procedures related to ISO / IEC 27001:2005 standard and is formally applicable to all organizations.
3. Identify and establish ownership-of or responsibility-for managing all information assets.
4. Carry out a review and manage information security risks associated with target activities and maintain continuity plan activities. Security risks are assessed at least once a year.
5. Conduct internal audits by an independent party at regular intervals to check compliance with policies, requirements, standards and procedures for information security, at least once a year.
6. Improve operational performance by evaluating the results of information security operations, assessing the level of compliance of information security framework and implementing any required corrective measures.
7. Working closely with departments and the relevant government agencies to improve the security of data and information exchange.

4.4.2.2 Leadership Responsibilities

1. Directly accountable for the consistency and effectiveness of information security management implementation within departments.
2. Make efforts to increase awareness of information security by disseminating this information security policy for all leaders and employees of the departments, related government agencies, business partners and other third parties who do the work / provide services to the KCG.
3. Improving the knowledge and skills of information security personnel through education, training, and socialization as needed.
4. Establish annual targets to be achieved by the process of managing information security, which is realized through the supervision and direction of the whole process of preparation and implementation of an information security work program on an on-going basis, which is intended to maintain and enhance long-term effectiveness, by providing appropriate resources.
5. Ensure availability of all resources (human, facilities, and budget) needed to implement information security policies.

4.4.2.3 Documentation Information Security Management

1. KCG is committed to develop and maintain documentation of information security management that consists of policies, procedures, standards and records.
2. Documentation of information security management should be made available in all areas of operations and accessible to users who require them. They shall be updated, maintained and protected from unauthorized use.

4.4.3. Third Party Security

4.4.3.1 Third Party Access Security

Access to information assets within KCG must be strictly controlled. Before providing access to partners, service users, departments / other agencies involved or other third party, the associated risks in connection with the provision of access must be identified and evaluated such that adequate controls may be implemented to reduce the impact or prevent the occurrence of those risks.

The evaluation must cover the following aspects:-

1) Type of access required:
2) Physical access to the office, workspace or server room(s).
3) Non-physical access into the network, database and information system.
4) Reason and needs access:
5) To provide support to hardware and/or software.
6) Audit of information security.
7) Development of applications and information systems.
8) Access methods, such as access via local network or access via modem (dial in) or IP VPN facilities.
9) Controlling the risks related to granting access to a third party must be specified in clearly-defined clauses and Non-Disclosure Agreement/NDA.
10) Contractual agreements with third parties must include, among others:
11) Third party liabilities are in compliant with information security policies enforced within the KCG.
12) Tacit agreement to comply with all policies related to the protection of information assets once access has been granted.
13) Type of access provided and procedure to use such access.
14) The identity of third-party employees who use this access.
15) Restricted locations where access can be done and time/period when the access may be used.
16) Confirmation of the right of KCG to monitor and control use of access.

4.4.3.2 Use of Third Party (outsourcing/sub-contract) by KCG Partners

Partners who employ third parties to provide services to the KCG or in carrying out either part or all of their work, shall ensure that all applicable KCG information security requirements are written in the contract agreement between the partners concerned and the service providers.
Contracts referred to in the clause above shall include:-

1) Assurance that all parties involved in the contract concerned are aware of their responsibilities to the security of KCG information assets.
2) Security controls, both physical and non-physical, must be applied to restrict access to information, and only to authorized employees / users.
3) Legal responsibility (legal aspects) of any information security breach during the delivery of services or in carrying out the work as stipulated in the contract.
4) The identity of resources involved in the contracted activities.

5) KCG shall ensure the availability of all resources (human, facilities, and budget) needed to implement information security policies.

4.4.4. Asset Classification and Control

1) All information assets and other assets associated with the security management of information are to be identified, recorded, valued and ascribed an owner. These assets include:-
   - Information assets - databases and data files, system documentation, user manuals, training material, operational or support procedures;
   - Software assets - application software, development tools and utilities;
   - Physical assets - computer equipment, communications equipment, magnetic media, site security;
   - Services - computing and communications services.

2) Each category of assets is to be recorded in an inventory. These inventories may be created in conjunction with other KCG business needs, e.g. business services, and/or as part of an overall KCG asset management system.

2) KCG information assets will have a protective marking (e.g. classification label), that reflect requirements for their Confidentiality, Integrity and Availability. These protective markings are to be ascribed in accordance with current KCG guidance.

4.4.5. Personnel Security

1) Security is to be an element of KCG's human resources management processes. Personnel security measures are required to reduce the risks to information systems arising from human error, theft, fraud or misuse of information assets.

2) KCG Senior Management, staff and staff of third party suppliers will undertake security vetting according to the value of the sensitive information they have access to in the course of their work. They will be required to sign a confidentiality/non-disclosure agreement with KCG.

3) The KCG Administration & Corporate Services departments will provide staff with security training as part of the induction process and as part of the user training for information systems. Input to security training material will be provided by other departments as needed. Security awareness will be programmed as a regular official activity. Third party suppliers will be required to demonstrate that their personnel security measures are consistent with the KCG security policy.

4) All KCG officials and members of KCG staff are to report all security related incidents to their line managers or though other specified channels as appropriate. Reporting is required of all security incidents, software malfunctions and suspected security weaknesses in systems or procedures.

5) KCG human resource management processes are to include procedures for handling employees who may have violated this information security policy or any of the security procedures, security manuals or other security related guidance documents.

4.4.6. Physical and Environmental Security

1) KCG physical security measures are to address risks to all KCG/Organization assets, including information assets.

2) There is to be particular focus on preventing unauthorized physical access to Office premises especially in any shared accommodation.

3) Physical and environmental measures to protect equipment are to take account of the risks of accident, everyday hazards of theft, fire, flood and power failures.

4) Remote workers shall ensure that the KCG information assets in their environment are adequately secured against misuse, loss, theft, and/or damage. They must use properly secured equipment for sensitive work. Guidance on this will be provided in security procedures.

5) Physical and environmental measures of third party suppliers are to meet KCG requirements and standards.

4.4.7. Communications and Operations Management

1) KCG requires comprehensive management of its communications and operations systems. Operating procedures for KCG information systems are to be documented and maintained. Change control processes are core to the proper management of information systems and these are to be fully documented.
2) Responsibilities for the proper operation of the KCG information systems are to be documented; duties are to be segregated as much as possible to reduce the risk of negligent or deliberate system misuse.
3) Software and procedural controls are to be in place throughout KCG information systems to minimize the risk of intrusion of a virus or malicious software.
4) The connections to KCG electronic information systems from systems owned by other agencies are to be protected in collaboration with the other departments.

4.4.8. Controlling Access to Information

1) KCG business needs define the access requirements for KCG Senior Management and staff to information systems. KCG information system users will be grouped into user groups for the purpose of managing access to KCG

information systems. The need-to-know principle will underpin all KCG access management procedures.

2) User accounts are to be created for users of KCG information systems. These are to be reviewed regularly by administrators to ensure that authorization processes remain sound, including effective passwords; in particular administrators are to check that all user accounts are actively required.
3) Access to all KCG networked or standalone computer services, and intelligent network devices, is to be via a secure log-on process designed to minimize the opportunity for unauthorized access. Each user of a computer system must be uniquely identified to the system. Where passwords are used, they will be managed in a secure manner to ensure their confidentiality and integrity. The process of authentication of a user to a system will include allocation of access rights to the data and facilities needed by the user's business role.

4) Users' access to data will be controlled and monitored in order to demonstrate conformance with the requirements of the information security policy.
5) Access control measures for users' remote electronic access and contractor remote diagnostics are to be robust in accordance with the security requirements of the KCG security policy.
6) Access control measures for system administrators are to be particularly robust to reflect the privileged access they will have to KCG information systems. Particularly strong physical, environmental and personnel security measures are to be used in support of access control measures for system administrators.
7) Electronic KCG systems security measures are to include timed lockout processes for inactive terminals.
8) Users' activities on KCG information systems will be audited in accordance with current KCG guidance in order to ensure conformance with the security policy.

4.4.9. Procurement, development, and maintenance of information Systems

1) KCG systems will be developed in such a way that security is a fundamental element of the development project in accordance with KCG information security policy and procedures. Development of an appropriate and agreed security regime will be integral to any proposal from a third party supplier for a KCG information system.

2) KCG shall clearly define and document security requirements of relevant information prior to construction, expansion, or procurement of a new information system.

3) The security of all KCG systems being developed will be subject to an accreditation process and a third party security health check to ensure that appropriate security measures are provided.

4) Information concerning the development of the information system for KCG will be confined to KCG staff and third party suppliers. Information concerning the

development of system security measures will be confined to KCG and third party suppliers' staff that have a need to know.

5) All aspects of any required cryptographic and encryption key management will be undertaken in accordance with KCG standards and procedures.

6) Each software package developed by third parties (partners or other third party) used in KCG's information systems must be free from deactivation mechanisms that can be triggered by external partners or other third party without the knowledge of KCG.

7) Technical vulnerabilities in KCG information systems must be identified, their risks assessed and controls established to prevent their exploitation or effectively resolve the weaknesses.

4.4.10. Information Security Incident Management

1) Disturbance/security incidents are evaluated periodically to ensure effective management, examine preventive measures that have been done, and plan how early detection of the incident.
2) Security weaknesses could result in imposition of disciplinary measures/sanctions to the staff responsible for the weaknesses.

3) Every computer user, whether employees, partners or third party personally responsible for ensuring that his actions did not cause or potentially cause security vulnerability information.

4) KCG must provide working tools to follow up and resolve any reported information security incidents quickly and effectively.

5) Information Security team should evaluate the report and completion of information security incidents to identify the type, volume and costs related to monitoring and performance evaluation purposes.

6) All data and records necessary to analyses and resolve information security incidents shall be secured. Records of incidents associated with civil or criminal actions, shall be secured/protected in line with applicable laws and regulations.

4.4.11. Business Continuity Management

1) Business Continuity Management will ensure that the highest priority KCG and other high priority official activities are able to continue whatever damage impacts KCG information assets.

2) A framework of business continuity plans will be produced for KCG. These plans will be regularly tested and kept under periodic review commensurate

with prevailing threats to KCG assets and changes in the KCG business environment.

3) Appropriate system and data backups will be undertaken, securely stored, and periodically tested, to ensure minimum disruption to business processing in the event of an incident requiring systems and or data to be restored to a position prior to the incident. Data back-ups will be taken at least once every 24 hours of normal working operation and stored securely off site.

4) KCG has developed an ICT Service Continuity Management Policy for the whole process of service-related activities vital to reduce the impact of ICT-based information systems failures or disasters that can affect the activities of KCG.

5) To ensure that Business Continuity Management remain relevant and effective, all recovery plans shall be tested regularly, at a minimum once a year. The results of these tests shall be analyzed and any faults in the plans shall be corrected.

4.4.12. Compliance

1) All KCG users are required to comply with all relevant legal statutes, licensing agreements, and KCG Policies.

2) KCG ensures that any provisions of law and legislation relevant to information systems owned by the KCG will be identified, documented and maintained.

3) KCG retains the right to access and review any document or file stored on KCG equipment and shall do so to ensure that no policy, agreement, or legal statute is contravened. Such review will be performed with the authority and knowledge of relevant officials under guidelines produced for monitoring conformance with the KCG data access policy.

4) Only authorized users shall have legitimate access to e-mail and Internet facilities provided by KCG. Limited personal use shall be permitted but all use must be in accordance with the Acceptable Use provisions of the KCG ICT Strategy and is not to include distasteful, derogatory or obscene material. Unauthorized access to pornographic or other sites containing offensive material or other serious misuse will result in KCG instituting disciplinary proceedings.

5) There will be a usage policy as part of KCG human resource management processes. This standard will address KCG users' use of e-mail and Internet both to reduce security risks and to ensure that users conform to KCG acceptable use policies of proper use of KCG information systems. This standard will also inform users that KCG will routinely monitor system usage to ensure user compliance with this standard.

6) All software installed on KCG computer system shall be properly licensed. Unauthorized copying of KCG -owned software is not permitted and is a violation of KCG copyright policy and provisions. Periodic inspection of installed software licenses will be made to ensure this standard is implemented effectively.

7) All creative ideas and discoveries by KCG employee during his/her employment, and produced by resources owned by the KCG, are to become the exclusive property of KCG.

8) Important records used or generated by information systems / information assets managed by KCG (databases, audit logs, transaction logs) should be protected from loss, damage or abuse, in line with applicable laws/regulations.
9) Third-party access to information processing facilities owned or managed by KCG may only be granted to personnel with appropriate level of competence, and complying with KCG information security policies.

10) All employees of the KCG, partners and other third parties are prohibited from using vulnerability scanning software or any software that would circumvent system security mechanism without formal authorization from KCG ICT Director.

4.5. Data Back-up

4.5.1. Preamble

ICT department shall manage, operate, and support a large number of computer systems throughout the KCG. In the event of any of these systems encountering data loss, each system should be covered by a data backup regimen.

The data backup regimen is a system of recording identified data onto portable media. This media is then stored both on-site and off-site to limit total loss in case of a declared disaster. The media contains a copy of specific data as at a specified time. The backup regimen is developed in conjunction with the client to meet both business and legislative requirements.
If that data is required for recovery, a data restore may be performed from the back up media.
This standard does not apply to personal devices including desktops, laptops, PDAs and USB storage devices such as USB hard drives and USB sticks. The backup and recovery of data on these devices is the responsibility of the individual user.

4.5.2. Data Backup Schedule

All computer systems operated, managed and/or supported by the ICT Department are covered under a Service Level Agreement (SLA). The SLA contains a proviso for the client's computer system – ensuring continuity of data access and protecting the client from data loss due to systems failure, virus, vandalism, operator error, or accidental erasure.

Where a SLA covers a computer system, and a backup regimen has been requested for that system, then the system is included in the data backup schedule. Prior to including the computer system in this schedule, the client will have determined which components and data they require to be backed up as per business and legislative requirements, which could include conducting a business risk assessment, which is dependent on:-

- Importance of the data and information to the organization;
- Acceptable transaction loss (business areas must determine what level of potential transaction loss would not be acceptable or would be too difficult to recover. This can be determined in terms of a timeframe, the number of transactions, or the amount of time and effort required re-entering data);
- The maximum acceptable outage of the system while performing backups;

A
n
d

- The maximum acceptable outage of system while recovering data.

4.5.3. Back-up Components

The following are the components of a back-up regimen for a computer system.

Data to be backed up may include:

Data Type	Description
Business Data	Memos, documents, customer information, financial records, databases, accounting information, project data, schedules and appointments, e-mail, and other critical files.
Systems Data	Software and hardware configuration data, software applications, user Ids, access rights, directory structures, passwords, e-mail configurations, and any other specialized systems information.

4.5.3.1 Backup Types and Frequency

All backups occur in line with a planned Data Back-up Schedule created by the ICT department to meet client requirements. There are three types of back-ups:

Back-up Type	Description
Full back-up	A complete copy of a computer system.
Incremental back-up	A copy of only the data updated since the last full or incremental backup.

Image copy	Where a computer system is virtualized, a copy of the virtual server is backed up.

Each of these back-up types may be performed at different frequencies or in combination:-

- Daily
- Weekly
- Monthly
- Quarterly
- Yearly

Typically, data back-ups are performed:

- Daily: for data that changes on a daily basis.
- Per an established schedule: for data that changes at scheduled intervals, or to respond to major system events.
- At month, quarter and year end: for systems with closing dates.

4.5.3.2 Media, Equipment, and Utilities

All media, equipment and backup utilities (backup management software and in-house programs) used to perform backups are tested prior to live use. This testing determines compatibility with computer systems, storage environment, and backup frequencies.

- Where media is found to be faulty after specific testing, media is replaced.
- Vendor contact details for support and maintenance of backup hardware is on hand to ensure service contingency.
- Backup utilities are supported either by the ICT department or vendor staff to ensure correct operation and backup success.

4.5.3.3 Storage

Backup media is stored both on-site and off-site. On-site storage is located within a physically secure and fire-proof area of KCG.

Off-site storage is in a secure and monitored location physically distant from t h e s o u r c e location premises. Authorized ICT department employees have 24x7x365 access to this location.

All media is securely stored whether in the on-site or off-site location, or in transit. Media is not stored in any location other than those authorized by the ICT department

4.5.3.4 Back-up Media Disposal

Obsolete backup media will be disposed of in a safe and secure manner in accordance with the Archived Data Retention and Disposal Schedule.

Back-up media to be disposed of must be rendered unreadable through an appropriate means. An audit-trail of disposal of back-up media will be maintained.

4.5.3.5 Backup and Recovery Documentation

Back up documentation should include the following items necessary to perform essential tasks during a recovery period:-

- Identification of all critical data, programs, documentation and support items;
- Clear documentation on how to do the backup and restore;
- Specified period of maximum acceptable outage (MAO) for all systems;
- Backup media storage locations;
- Required backup frequency, e.g. daily, weekly;
- Required backup cycles;
- Backup retention period (as per business and legislative requirements);
- Testing regimen and process;
- Recovery schedule and plan; and
- Location of relevant software and licenses.

Back-up and recovery documentation will be reviewed and updated regularly to account for new technology, business changes, and migration of application to alternative platforms.
Documentation of the restoration process will include procedures for the recovery from single- system or application failures as well as for a total data center disaster scenario.

4.5.4. Data Restoration

All back-up data is accessible through data restoration. Data restores are performed within a physically secure area of ICT Department employees. Restores are performed using tested utilities.
Before a restore is initiated, the client will have specified which files are to be recovered, and where those files are to be placed.
Client requests for data restores are only undertaken where the request is authorized by client management.

4.5.5. Quality Assurance and Exceptions

On the completion of a backup, success is verified using a backup log that monitors the files being backed up? Designated ICT department employees check backup logs on a regular basis as part of their standard duties.

Backup successes and failures are noted in a Backup Status Log. All failures are investigated, and any problems corrected in accordance with the terms of the SLA.

By default, every backup should complete with a data capture of 100% success rate. This standard is vital to the principle of quality data access continuity in the event of the need for a data restore.

4.5.5.1 Exceptions

Although the back-up success rate should be 100%, there are allowable exceptions to the rule. A back-up may fail either partially or fully in the event of a major power

failure, a major power surge, because the files are in use or hardware and software failure.

4.5.5.1.1 Major Power Failure

A major power failure may lead to systems being powered by the Uninterruptible Power Supply (UPS). However, the UPS is not designed to provide maximum and indefinite use. The source computer system containing files scheduled for back-up may have to be shut down during an outage, and/or the outage could affect the computer system driving the backup device. Both cases would make it impossible to perform a data backup at that time.

4.5.5.1.2 Major Power Surge

Although greatly reduced due to the presence of the UPS, a major power surge could damage either the source computer system or the system driving the backup device.

4.5.5.1.3 File in Use

Some computer systems require that no file is accessed or open during a backup. Where a client is using a file, rendering it unable to be backed up, and the result is the client's responsibility. This includes access by authorized representatives and unauthorized persons through the fault of the client.

4.5.5.1.4 Major Power Failure

A major backup hardware or software failure may lead to backups not being completed or performed. In this situation, if appropriate, the backups will be rescheduled.

4.5.5.2 Backup and Recovery Verification

Backup and Recovery procedures will be tested and verified on regular basis or as required.

4.5.6. Responsibilities

ICT Department has responsibilities in respect of data back-ups.

4.5.6.1 KCG ICT Department Responsibilities

ICT department should be responsible for:-

- Configuring a fully tested backup system (including media, equipment, and utilities) and data restoration capabilities;
- Securing a comprehensive vendor support and maintenance contract (Including replacement);
- Ensuring all data that KCG departments have requested to be backed up is backed up in accordance with the client's SLA;
- Initiating, managing, and monitoring all data back-ups;
- Reporting back-up successes and failures to the client on the basis and frequency agreed to in the SLA;

- Ensuring all back-up failures are investigated and examined to ensure process integrity;
- Ensuring all faults affecting backup integrity are addressed within the agreed support timeframe documented in the SLA;
- Formulating and documenting support, guidance, and operational policies, processes, and procedures in support of all back-up activities;
- Secure storage of media within KCG and at the off-site storage facility;
- Ensuring all client data is inaccessible to unauthorized persons;
- Modifying backup characteristics/requirements when formally requested by KCG departments;
- Notifying KCG departments as far in advance as possible of any changes affecting the department's backup (e.g. time, quality, frequency etc.); and
- Ensuring that backup media is rendered unreadable prior to disposal and media is disposed of in an appropriate manner.

4.5.6.2 KCG Departments Responsibilities

KCG departments, and any authorized representative of the departments, are responsible for:-

- Accurately identifying and documenting all data to be stored in their backups in accordance with business and legislative requirements;
- Notifying the ICT department (via the procedure documented in the SLA) of the required backup regimen, and of any changes to that frequency. Ensuring the backup regimen meets all business and legislative archival requirements;
- Requesting the ICT department to perform a data restore via the channels documented in the SLA; and
- Ensuring all files are free and available for backing up at the scheduled time.

4.5.6.3 Exceptions

The details in this standard may be amended under the following exceptional circumstances:-

- By specific agreement as formalized in the client's SLA; and
- By special request of the ICT department and.

4.5.7. Data Archiving

All electronic data should be archived with the Ministry of Administration, Corporate Services & Stakeholder Management.

No data should be destroyed without the written approval of the above.

4.6. ICT Audit

4.6.1. Preamble

In line with rapid advancement of technology most governments have become increasingly reliant on computerized information systems to deliver public services and carry out their daily operations. As a consequence, the reliability, integrity and

availability of computerized data and of the systems that process, maintain and report these data are a major concern to audit. ICT Auditors examine the adequacy of controls in information systems and related operations to ensure system effectiveness.

ICT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively, and uses resources efficiently.

ICT auditing is a branch of general auditing concerned with governance (control) of information and communications technologies (computers).

4.6.1.1 Controls in an ICT System

In order for any computer systems to work as they are designed, achieve results accurately, efficiently, and securely and perform within the specified constraints, they would need controls. These controls are of great value in any computerized system and it is an important task for an auditor to see that not only adequate controls exist, but that they also work effectively to ensure results and achieve objectives. Also controls should be commensurate with the risk assessed so as to reduce the impact of identified risks to acceptable levels.
Controls in a computerized information system reflect the policies, procedures, practices and organizational structures designed to provide reasonable assurance that objectives will be achieved.
Information system controls are broadly classified into two broad categories:

- General Controls
- Application controls

General controls include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. They create the environment in which the application systems and application controls operate. Examples include IT policies, standards, and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, service continuity planning, IT project management, etc.
Application controls pertain to specific computer applications. They include controls that help to ensure the proper authorization, completeness, accuracy, and validity of transactions, maintenance, and other types of data input. Examples include system edit checks of the format of entered data to help prevent possible invalid input, system enforced transaction controls that prevent users from performing transactions that are not part of their normal duties, and the creation of detailed reports and transaction control totals that can be balanced by various units to the source data to ensure all transactions have been posted completely and accurately.

4.6.1.2 Objectives of ICT Controls

As a principle, the objectives of internal controls remain unchanged with the introduction of ICT. It is the control techniques that change with many of the manual controls being replaced with automated processes and new technical controls added

to achieve the same objectives. Typical control objectives within a government ICT function are to ensure:

i. Provision of effective departmental organizational control over functions related to the use of ICT infrastructure by clearly defining organizational objectives;

ii. Effective management control over development of ICT infrastructure resources in accordance organizational objectives;

iii. Operational management of ICT infrastructure in accordance with statutory requirements and industry good practices;

iv. Formulation of an adherence to policies, standards and procedures for all functions related to ICT infrastructure and

v. Efficiency and effectiveness of the ICT infrastructure systems towards achievement of its desired objectives.

4.6.1.3 Controls Based on Domains

Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

Technical security controls (also called logical controls) are devices, processes, protocols, and other technology-based measures used to protect sensitive information.

Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.

4.6.1.4 Controls Based on Purpose

Directive security controls are the equivalent of administrative controls. Directive controls direct that some action be taken to protect sensitive organizational information. The directive can be in the form of a policy, procedure, or guideline.

Preventive – security controls that are put into place to prevent intentional or unintentional disclosure, alteration, or destruction of sensitive information. Notice that preventive controls may also cross-administrative, technical, and physical categories as discussed previously. The same is true for any of the controls discussed in this section.

Detective security controls have the function of providing an alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred, either manually or automatically. Example detective security controls are log monitoring and review, system audit, file integrity checkers, and motion detection.

Note that in some cases, Detective controls are complemented with a **Delay** mechanism – to prevent an attempt for unauthorized access from being able to progress immediately.

Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. Note that in many cases the corrective security control is triggered by a detective security control. A corrective control will essentially include **Assess** and **Respond** phases.

Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category.

4.6.1.5 Other Control Types

Deterrent security controls are controls that discourage security violations. For instance, "Unauthorized Access Prohibited" signage may deter a trespasser from entering an area. The presence of security cameras might deter an employee from stealing equipment. A policy that states access to servers is monitored could deter unauthorized access.
Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason (e.g. operational or technology constraints).

4.6.1.6 ICT Audit Standards

- ISACA COBIT v4.2 – COBIT (Control Objectives for IT) is a framework created by ISACA for information technology (IT) management and IT Governance. The framework provides good practices across a domain and process framework. The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate) and 34 processes in line with the responsibility areas of plan, build, run and monitor.

The use of COBIT in any audit program should be done sparingly – certain areas of COBIT should be selected to reflect the target organization's maturity in ICT management and whether certain controls are indeed relevant for that organization. A good start in using COBIT is in a maturity assessment process, where applicable controls are evaluated for its maturity and non-relevant controls are identified with suitable analysis. An auditor can then use this result to plan which areas of high risk should be focused for subsequent planning.

- ISO/IEC 27001:2005 Information Security Management – is the international standard for Information Security Management System and along with ISO/IEC 27002 (Guidelines) describes a complete framework of how information security management should be implemented in an organization. The standard defines management and technical controls, the latter with sufficient detail (39 Control Objectives and 133 Controls). Departments wishing to obtain a certification based on this standard may do so by appointing a suitable Certification Body to conduct a certification audit.
- ISO/IEC 20000:2005 IT Service Management – is the international standard for IT Service Management that describes how IT *as a service* should be managed. The ISO/IEC 2000x series provide a comprehensive definition of an IT Service Management framework and similar to the ISO/IEC 27001 standard, may be adopted for the purpose of obtaining an external Certification.

4.6.2. General ICT Audit Policy

1. ICT Audit aims to provide recommendations for improvements related to any control weaknesses.
2. ICT Audits can be conducted as a stand-alone activity or be part of a general audit.

3. The audit is based on a formal charter (audit charter). The Audit Charter shall contain at least:

   a. The purpose of the audit b. Scope of audit
   c. Authority of the auditors
   d. Auditors' Liability
   e. Auditors' responsibility
   f. Reporting of audit results

4. IT Audit shall be based on current KCG regulations on ICT and on the following standards and frameworks:

   - ISACA COBIT v4.2
   - ISO/IEC 27001:2005 Information Security Management
   - ISO/IEC 20000:2005 IT Service Management

5. Auditors should uphold professional and organizational ethics.

6. In all matters relating to audit activities, the audit unit should be independent and objective.

7. The auditor must have professional competence and ability to perform the tasks of information technology audit.

8. Auditors should prepare audit plans and procedures based on a risk-based approach. Results of risk assessments are to be used to set priorities and allocation of audit resources.
9. In the implementation of audit, the auditor should:

    a. Able to ensure the audit objective is achieved according to professional auditing standards;
    b. Gather sufficient evidence that can be trusted, and relevant to support its findings; and
    c. Document the audit process and audit evidence to support his conclusions.
10. Auditors shall also examine general IT controls for their performance (effectiveness and consistency). General controls include but are not limited to:
    a. Policies and procedures for information and communication technology security;
    b. Separation of duties;
    c. Conformance to information system development policies (system development life cycle);
    d. Changes to ICT environment and the change management process; and
    e. Business continuity preparedness.
11. Meanwhile, the control applications include but are not limited to:

    a. Identification, authentication, and authorization;
    b. System interfaces;
    c. Accuracy and completeness of transaction processing; and
    d. Logging and audit trail.
12. If auditors find a weakness or inconsistency that is material in nature related to any controls, the auditor should communicate the issue to the appropriate level of management in a timely fashion.

13. Auditors must provide full and comprehensive report after the completion of audit process. This report must contain at least:

    a. The purpose of the audit;
    b. The scope of the audit;
    c. The period of audit;
    d. Audit findings, conclusions, and recommendations;
    e. Limitations and constraints encountered in the audit process;

f. The procedure for distribution of reports according to the provisions of the Charter of the Audit.

14. Auditors may request assistance from external professionals to conduct the audit. Prior to employing external expert assistance the audit supervisor shall ensure that the outside personnel have the required skills, competence, professional qualifications, relevant experience, and independence.

15. After reporting the findings and recommendations, the auditor should monitor all findings to ensure audited implements corrective measures effectively.

Table 1: Segregation of Duty Conflict Matrix

	DBA Staging	DBA Production	System Administrator Staging	System Administrator Production	Manager	Software Developer	Security Officer	Use
Uses Application	X	X	X	X	X	X	X	
Initiates Change			X		X			
Authorizes Change	X	X		X	X	X		
Tests Updates – Database		X		X	X	X	X	
Tests Updates – Application	X	X	X	X	X	X	X	
Implements Updates – Database	X		X	X	X	X	X	
Implements Updates – Application	X	X				X	X	
Access to Source Code		X		X	X		X	
Administrative Access – Database O/S Staging		X	X	X	X	X		
Administrative Access – Database O/S Production	X		X	X	X	X		
Administrative Access – Application O/S Staging	X	X		X	X	X		
Administrative Access – Application O/S Production	X	X	X			X		
Administrative Access – Staging Database		X	X	X	X			
Administrative Access – Staging Application	X	X		X	X			
Administrative Access – Production Database	X		X	X	X	X		
Administrative Access – Production Application	X	X	X			X		
Monitors Changes and Security Events	X	X	X	X	X		X	

Note: Cells marked with an "X" indicate roles and tasks that are incompatible with each other, and where segregation of duties is advised.

4.6.3.2.2 Physical Access Control

Physical access controls include controls against environmental threats, which operate across the whole ICT environment and affect all underlying systems. These controls are designed to protect the system hardware and software from damage, theft and unauthorized access. Restricting physical access to the ICT systems reduces the risk of unauthorized persons altering the financial information. During an audit, ICT Auditor should conduct assessment of physical access controls throughout the whole audit programme, by observations of how these controls are being implemented within areas/facilities under review, as well as by taking samples of control records.

4.6.3.2.3 Authorization Control

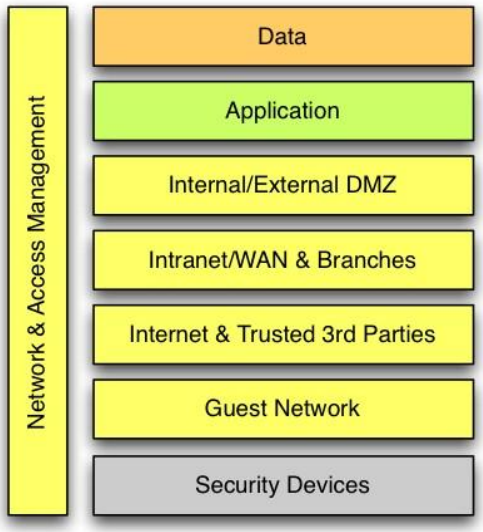
Authorization control helps verify the identity and authority of the person involved in executing a procedure or an operation. This control is exercised through the use of passwords, signatures, smart cards, cryptographic systems etc. Such-controls ensure that only an authorized person has access to the system and its use, to enter and/or alter transactions, to take information etc.

In critical systems, authorization controls may take the form of multiple layers of preventive (prior authorization and verification of identity before issuing system access) and detective (regular review of user access), designed to provide a fail-safe mechanism. When auditing, it is important to analyze how a failure in one or more authorization controls may affect the security of the system being protected.

4.6.3.2.4 Logical Access control

Logical Access controls are provided to protect the critical applications and underlying data files from unauthorized access, amendment or deletion. Logical access controls can exist at both an installation and application level. Controls within the general ICT environment restrict access to the operating system, system resources and applications, whilst the application level controls restrict user activities within individual applications.

Logical access controls can also be used to restrict the use of powerful systems utilities, such as file editors and system configuration panel. Logical access controls are often used with physical access controls to reduce the risk of the programs and data files being amended without authority. The importance of logical access controls is increased where physical access controls are less effective, for example, when systems make use of communication networks (LANs and WANs). The existence of adequate logical access security is particularly important where a client makes use of wide area networks and global facilities such as the Internet.



Implementation of layered controls should be defined based on access requirements and risks related to each access type. The figure above illustrates how various layer of controls should be applied logically to protect access from different user profiles.

The most common form of logical access control is login usernames followed by password authentication. For passwords to be effective there must be appropriate password policies and procedures, which are known to all staff and adhered to. Menu restrictions can be effective in controlling access to applications and system utilities.

Systems may be able to control access by identifying each individual user through their unique login ids and then having a pre-defined profile of authorized menus for each. The ICT Auditor should consider how easy it would be for users to 'break out' of the menu system and gain unauthorized access to the operating system or other applications. Some computer systems may be able to control user access to applications and data files by using file permissions. These ensure that only those users with the appropriate access rights can read, write, delete or execute files.

4.6.3.2.5 Change Management Controls

Change management controls are used to ensure that amendments to a system are properly authorized, tested, accepted and documented. Poor change controls could result in accidental or malicious changes to the software and data. Poorly designed changes could alter critical information, introduce system malfunction and remove audit trails. Audit should ensure that a new or amended system is thoroughly tested by its end users before operational implementation. These regular changes may be necessary to improve efficiency, functionality or remove programming faults ('bugs').

ICT Audit should emphasize that auditee organizations have an appropriate change management and configuration management controls. Configuration management procedures relate to the control of ICT assets and the subsequent update of records, whilst

change management relates to the authorization, impact assessment, asset update, testing and implementation of changes.

4.6.3.2.6 Network Communication Security Controls

Network communication security controls are critical when LANs/WANs or web enabled systems are in use. Some important aspects to be covered by this control are as follows:

i. All sensitive information processed (transmitted) within the network should be protected by using appropriate techniques;
ii. Critical network devices such as routers, switches and modems should be protected from physical damage;
iii. Network configuration and inventories should be documented and maintained;
iv. Prior authorization from Network Administrator should be obtained for making any changes to the network configuration.
v. Any changes made in the network configuration should be documented. The threat and risk assessment of the network due to these changes in the network configuration should be reviewed.
vi. The network operation should be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.
vii. Physical access to communications and network sites should be controlled and restricted.
viii. Communication and network systems should be controlled and restricted to authorized individuals.
ix. Network should be monitored using diagnostic tools by authorized personnel.
x. Network perimeter security should be used to isolate an organization's data network from any external network. Networks that operate at varying security levels should be isolated from each other by appropriate firewalls. The internal network of the organization should be physically and logically isolated from the Internet and any other external connection. All network security devices should be subjected to thorough testing for vulnerability prior to implementation and at least half-yearly thereafter. All web servers for access by Internet users should be isolated from other data and host servers.
xi. Connectivity with third parties should be implemented with suitable security controls. KCG should establish procedures for allowing connectivity of their network or application system to any third parties. The permission to connect other networks and application system should be based on clear purpose (regulation, government policy) and approved by the Network Administrator and documented. All unused connections and network segments should be disconnected from active networks. Any systems accessing KCG's host system must adhere to the general system security and access control guidelines. The suitability of the protocol used for third party connections should be assessed prior to ensure compatibility and protection of data exchange. The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

xii. The responsibility of technically managing each system shall be allocated to a properly trained System Administrator, who is then responsible for operation, monitoring security and functioning of the system.

xiii. Any reports of unusual activity or pattern of access on the computer network should be investigated promptly by the Network Administrator. The system must include a mechanism for alerting the Network Administrator of possible breaches in security,

4.6.3.2.7 Business Continuity Planning

Each department should have an established plan to guard against disastrous events and ensure the continuity of public services (See related ICT Security Policies on Business Continuity Planning). The auditor should verify that there are adequate plans to resume processing in the event of complete failure of computer operations. The degree of continuity planning will depend on the size of the ICT department and the dependence of critical business processes on computer processing. Disaster recovery planning for ICT facilities should be treated as one element of KCG's overall business continuity plan.

The extent of disaster recovery planning and the detailed measures required will vary considerably. KCG, with multiple business systems and complex communication networks may require comprehensive, up to date recovery plans which incorporate standby facilities at alternative sites.
Disaster recovery plans should be documented, periodically tested and updated as necessary. Untested plans may be satisfactory on paper but fail when put into practice.

Testing will reveal deficiencies and allow amendments to be made. The importance of adequate documentation is increased where significant reliance is placed on a few key members of the ICT department. The loss of key staff may adversely affect KCG's ability to resume operations within a reasonable timeframe.

Back-up copies of systems software, mission critical applications and underlying data files should be taken regularly. Back-ups should be cycled through a number of generations by, for example, using daily, weekly, monthly and quarterly tapes. Back-ups should be stored, together with a copy of the disaster recovery plan and systems documentation, in an off- site fire-safe. Where end-user computing processes are used, in addition to centralized application systems, the auditor should ensure that there are also procedures for the backing-up of critical data stored on local hard disks.

4.6.3.3 Evaluation of General Controls

When reviewing general controls, the following areas should be covered:

i. Evaluation of ICT Asset management by acquiring a list of asset including, computers, ancillary and terminal equipment in use indicating model, performance details and verify the existence of this equipment – in many current implementation, a CMDB (Configuration Management Database) may be available for examination;

ii. Analyzing ICT Management structure in the organization by acquiring a current organizational chart and analyze how computing facilities are used/managed within the overall KCG. The analysis should be extended to cover how the ICT Management

structure is staffed by using up-to-date personnel chart of the ICT department showing the roles, responsibilities and authorities –ensure that all critical operational and governance roles are allocated;

iii. Examine whether operational procedures are in line with established practices by using the details of standards and operational guidelines that have been defined for each of the ICT functions, like data control, data preparation, system operation and verify that they have been implemented consistently. Also confirm that operational manuals are maintained and kept up-to-date, specifying the control procedures and whether they are enforced in practice through regular evaluations

iv. Verify the existence of the following terminal controls to protect data and system integrity:

a. physical access controls to terminal rooms;
b. user authentication controls through password protection and user directories;
c. logging of terminal activities by all users.

v. Evaluate the effectiveness of physical security controls to protect against risk of man-made disasters. Examples of suitable controls are:

a. Fire prevention controls (fire prevention steps, detection mechanism and firefighting arrangements);
b. Regular maintenance of computer and related equipment;
c. Environmental control system (air conditioning) and protection against possible radiations, vibrations;
d. Human resource controls for possible industrial action, malicious action by programmers, operators, and temporary staff;
e. Security awareness and training programmes provided to all employees;
f. Emergency shut-down procedures in case of power failures;
g. Chain of custody of software, data files and tape library;
h. Adequacy of back-up files (offsite storage included);
i. Restricting operator access to program files and data;
j. Procedures for reconstructing files in the event of loss or disk errors/tape errors (contingency plans);
k. Back-up for computer equipment failure through the use of compatible equipment at other dispersed sites;
l. Data Centre's, Server Rooms and Data Communication Rooms should be off limits to all except systems operators, hardware engineers and
m. Insurance policy of the installation to cover possible risk (if available).

4.6.3.4 Application Controls

Application control mechanisms are largely specific to an application and have a direct impact on the way individual transactions is processed. These controls are implemented to provide assurance that all transactions are authorized, valid and recorded. Since application controls are closely related to individual transactions the audit will provide the auditor with assurance as to the level of accuracy of a particular data file.

Prior to conducting and evaluation of application controls, it will be necessary to ensure a suitable understanding of the application system;

i. The business process done through the application, including inputs, outputs and interfaces with other processes/systems;
ii. How data is to be managed within the applications, including volume of transactions and data stored;
iii. Technology platforms used and how they are configured.

4.6.3.4.1 Audit Requirements

When auditing an ICT infrastructure that are complex or involving multiple technology platforms, the auditor shall identify pre-requisite conditions to ensure that the system can be audited in an effective and efficient manner.

4.6.4. Audit Methodology

4.6.4.1 Types of ICT Audits

An audit programme is usually developed for particular reason – this can be an annual audit to cover the entire KCG, or specific audit conducted to focus on certain issues of interest. The former is clearly of such magnitude that audit units usually derive an annual audit programme to allow wide-ranging areas to be covered so as to provide overall status of compliance to management.

In most cases, the annual programme will have to include specific in-depth audit to be done on certain initiatives that may be related to on-going strategic initiatives or to examine level of compliance to new regulations. For reference, the following types of ICT audits may be used singly or in multiple combinations, to help define an audit programme:

- Operational computer system/network audits: review the controls within and surrounding operational computer systems and networks, at various levels e.g. network, operating system, layered software, application software, databases, logical/procedural controls, preventive/detective/corrective controls, crypto, system logging.
- ICT installation audits: examine the physical aspect of the computer building, server rooms, network/communication cupboard, including aspects such as physical security (walls, CCTV, locks, guards, barbed wire, visitor procedures), environmental controls (fire and flood protection, power supply, air conditioning), computer and network operations processes and management systems.
- Systems development audits: typically cover either or both of two aspects: (1) project or programme management controls); and (2) the specification, development, testing, implementation (installation and configuration) and initial operation of technical and procedural controls, including classical technical information security controls and the related business process controls such as divisions of responsibility. See further discussion on this below.
- ICT management audits: review the organization, structure, strategy, work planning, resource planning, budgeting, cost controls etc. and, where applicable, relationships with outsourced ICT providers.
- ICT process audits: review the processes which take place within IT department such as application development, testing, implementation, operations,

maintenance, housekeeping (backups, preventive maintenance etc.), support, incident handling.

- Change management audits: review the planning and control of changes to systems, networks, applications, processes, facilities etc., including configuration management, control over the movement of code from development through testing to production, and the management of changes to KCG as a result of ICT.
- Information security & control audits: review controls relating to confidentiality, integrity and availability of systems and data.
- ICT legal compliance audits: review legal and regulatory aspects of IT systems (e.g. software copyright compliance, protection of personal data).
- Certification and other compliance audits: compliance audit based on information security standards such as ISO/IEC 27001 and industry standards such as PCI-DSS. Formal certification audits typically have strictly defined scopes.
- Disaster contingency, business continuity planning and IT disaster recovery audits: review arrangements to restore some semblance of normality after a disaster affecting the IT systems, and perhaps assess the organization's approach to risk management, reviewing the links between (a) identifying and protecting critical business processes, and (b) securing the supporting IT services, systems, network and processes. These audits may or may not cover the much-neglected but vital issue of resilience, which is of course all about avoiding disastrous outages as far as possible.
- "Special investigations": contingency and other un-pre-planned audit such as investigating suspected frauds or information security breaches, performing due diligence review of IT assets for mergers and acquisitions etc.

4.7. ICT Project Management

4.7.1. Purpose

This standard provides an overview of the essential components of the project management methodology used within KCG.

This standard includes the 'what', 'when' and 'why' of project management methodology. Examples of 'how' can be found in supporting procedures and forms.

As a methodology, this standard provides a structured approach to managing projects with ICT components.

4.7.2. Scope

Most of the principles that apply to significant (medium to large) projects also apply to smaller projects. However, the extent to which these principles are applied will vary, depending on the complexity of the project.

A scaled down version of these standards and guidelines may be adopted to support the management of smaller projects.

The procedure: *Determining a Project Size* will assist in determining both the size of a project (small, medium or large) and the amount and type of documentation to be developed for each project size.

4.7.3. Guides, Procedures, Worksheets and Forms

The guides and procedures, standard templates and forms for use in implementing these standards and guidelines are those provided by Prince2 Project Management methodology.

4.7.4. Project Management

4.7.4.1 Definition

A project involves a group of inter-related activities that are planned and then executed in a certain sequence to create a unique product or service within a specific time frame. Projects are often critical components of an organization's business strategy, or relate directly to policies and initiatives of the organization.

Projects vary in size or complexity, for example they may:

- involve changes to existing systems, policies, legislation and/or procedures
- entail organizational change
- involve a single person, or many people
- involve a single unit of the organization, or may cross organizational boundaries
- involve engagement and management of external resources
- cost anywhere from Kes 1 million to more than a Kes 100 million
- Require less than 100 hours or take several years.

4.7.4.2 Essential characteristics

A KCG ICT project is characterized as having:

- Business Case
- definable, measurable project outcomes that relate to KCG goals
- project outputs (required for the attainment of the project outcomes) produced by a project team(s)
- project governance structure
- well-defined project team(s)
- Criteria to measure project performance.

The structure of a project will vary, depending on the benefits the project is intended to provide. To achieve these benefits, a project may need to be structured into a number of sub-projects.

4.7.4.3 Project management

Project management is the formalized and structured method of managing change. Project management focuses on achieving specifically defined outputs in a certain time, to a defined quality, and with a given level of resources, in order that specific outcomes are achieved.
Effective project management is essential for the success of a project.

4.8. Systems Development

4.8.1. Purpose

This standard defines what controls will be implemented by organizations in relation to

System Development and Maintenance.

This standard is consistent with, and should be read in conjunction with the Information Systems Security Guidelines.

This standard interprets current industry standards and recommends an application development standard for adoption in KCG for the software/application development lifecycle, consistent with enterprise architecture standards (in particular, compliance with the enterprise architecture checklist), principles, and best practices.

The application development standard will provide:

- Adequate Application Development Standards for all stages of the application development process
- Minimum requirements for application development activities, deliverables and acceptance sign-off
- A general measure for ensuring the application development methodology is in compliance with the application development standard.

4.8.1.1 Application of the standards

Each project will have different requirements and it is up to individual project teams to determine whether they will take a 'pure' or 'hybrid' approach combining aspects of various standards. Teams may adopt a hybrid standard if they think it will better serve the needs of the project, as long as the methodology is fully articulated and adhered to. The systems development standards are divided into the following.

4.8.1.2 Programming Standards

Project Teams are expected to maintain standards for the development of the application/software source code. Their purpose is to increase application/software quality, by proper commenting, limiting module complexity, systematic naming conventions, and other techniques. Such standards are often dependent on the choice of programming language.

4.8.1.3 Design Standards

Project Teams will also benefit from design standards. These can help ensure that consistent techniques are used, e.g. in conjunction with object-oriented design methods. Guiding principles, such as encapsulation and information hiding, may be defined, and checklists maybe developed for use in the design reviews.

4.8.1.4 Applicability statement

KCG IT Standards apply for use by all Project Teams. As new KCG ICT standards are approved, they are deemed mandatory on a go-forward basis (Go-forward basis means at the next available project development or procurement opportunity).

4.8.1.5 Requirement Levels

Within this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

Must	This requirement is not optional
May	The implementer *may* choose to take one or more of a selection of options, but *must* make a choice of one or more, as dictated within the context of
Should	The implementer *must* choose this action, *unless* business functionality dictates otherwise. Exceptions *must* be approved by management, as modifications to the standard practice

4.8.2. Application Development in an Organization

While various application development methodologies have been developed to guide application development processes, the key application development methodologies used within the organization are Waterfall and Iterative. Generally, the critical objectives, activities and deliverables of each of these methodologies remain the same. ICT department has undertaken the task to identify these various Systems Development Life Cycle (SDLC), and develop an application development standard that is applicable across various methodologies. Project Teams will use this standard to help guide application development in a consistent, standard and predictable manner.

Effective application development processes are critical to the success of IT projects. Project Teams must select and follow one of the application development processes that can be categorized as Waterfall or Iterative; however, this System Development Standard must be used within the organization to achieve compliance. This standard clearly defines expected application development activities, measures and deliverables for each phase to help in ensuring that the necessary standards are maintained through the entire life of the project.

PROJECT TEAMS MUST SELECT ONE APPLICATION DEVELOPMENT METHODOLOGY AND USE IT FOR THE DURATION OF THE ENTIRE PROJECT.

4.8.2.1 Waterfall SDLC

The waterfall model is a popular version of the software development life cycle model for software engineering. Often considered the classic approach to the application/software development life cycle, the waterfall model describes a linear and sequential development method with distinct goals for each phase of development.

4.8.2.2 Iterative Incremental SDLC

Iterative and Incremental Development is an application/software development process developed in response to specific weaknesses of the more traditional waterfall model.

The iterative process starts with architecturally significant subset of the application/software requirements (often the high risk requirements) and iteratively enhances the evolving sequence of versions until the full application/software is implemented. At each iteration,

design modifications are made and new functional capabilities are added. This allows the project team to take advantage of what was learned during the development of earlier, incremental, deliverable versions of the application/software. The product is defined as completed when it satisfies all of its requirements.

4.8.3. Application Development Standard

Application development shall follow the Waterfall model and the Iterative Incremental models. Team members may choose to use a hybrid of these models and other modern development methodologies.

4.9. E-Waste Management

4.9.1. Preamble

The *KCG ICT Standard for e-Waste* covers the collection and handling of waste ICT electronic equipment within the Government, taking into account appropriate environmental and sustainability factors.

For the purposes of this standard, electronic waste or e-Waste may be defined as all desktop computers, notebook or laptop computers, CD-ROM and DVD equipment, data projectors, digital cameras, telephones, mobile phones and personal digital assistants (PDAs), printers, photocopiers, fax machines and multifunction devices (MFDs), keyboards and similar peripheral ICT devices, servers, hubs, switches, bridges, routers, power supplies and batteries, UPS, scanners, electronic entertainment devices and consoles, and other similar items. This definition includes used electronic equipment destined for reuse, resale, salvage, recycling, or disposal. E-Waste is considered as waste at the point that the Government permanently discards the item of equipment from its ownership. The following principles will apply to the responsible disposal of e-Waste:

- Disposal, Data protection and Information integrity; and
- Environmental protection and Social responsibility.

The coordination of activities associated with the appropriate handling and disposal of e-Waste will be managed by the ICT department. Records will be maintained to document the amount of e-Waste disposed of each year in accordance with reporting requirements demonstrating compliance with environmentally friendly initiatives.

4.9.2. Standards

4.9.2.1 Disposal, Data Protection and Information Integrity

Disposal of KCG ICT assets and equipment, deemed as e-Waste, will be in accordance with procedures specified in these Standards. The ICT department make every effort to ensure maximum usage and value for money is obtained from all electronic items to ensure that e-Waste is minimized.

Only designated collection and disposal points will be used for e-Waste. NO electronic equipment and e-Waste will be placed in general refuse bins. Procedures for the safe handling and disposal of e-Waste will be available to the public.

Equipment that is to be disposed may hold sensitive information and licensed software applications. Provisions within the *KCG Standard for ICT Information Management and*

Security and the associated *KCG ICT Standard for Information Asset Classification and Control* will be followed to ensure that any personal or sensitive information has been removed from electronic storage media or such media is rendered unreadable and/or unusable. Where ownership of the equipment is to be transferred to a third party with the intention that the third party will continue to use the equipment, Organization responsible for ICT implementation or regulation in Kisii staff will ensure that the equipment only contains licensed software applications and operating systems that can be legally transferred with the equipment.

4.9.2.2 Environmental Protection and Social Responsibility

The KCG will not dispose of electronic equipment that is within its agreed lifecycle and continues to be supported by vendors under appropriate maintenance and warranty support agreements. E-Waste equipment shall be disposed of or recycled in an environmentally and socially friendly manner in accordance with the National Environmental Act. The ICT department will make all reasonable efforts to ensure that e-Waste equipment does not end up in landfills in Kisii.

4.9.2.3 ICT Procurement

The acquisition of environmentally preferable or 'green" goods and services is a key priority of the KCG ICT department, and the department will consider selection criteria for ICT goods and services that have a lower impact on the environment and the health and well-being of staff and the community and will be ethically and socially responsible when considering value for money.

4.9.3. User Education

The responsible disposal of e-Waste will become an important issue as ICT equipment usage continues to grow. Most staff are not fully aware of the range of hazardous materials used in the manufacture of ICT equipment and the requirement for special disposal of such equipment so that adverse environmental damage does not occur. Most staff and members of the wider community are becoming more environmentally conscious and will recycle and dispose of ICT equipment responsibly if they have appropriate information.

Addressing the responsible removal of e-Waste and recycling requires user education programmes to be incorporated into staff induction and development activities to ensure that it becomes part of the culture at KCG. The ICT department will develop material and education programs that will be published on Kisii County website and delivered in person to all staff during basic ICT training sessions.

4.10. Strategic and Operational Planning

4.10.1. Preamble

This standard is intended to identify the various processes and activities performed within the KCG that influence the allocation of ICT resources towards ensuring projects and activities are aligned to achieving the business requirements of KCG.

This standard has been put in place to ensure that ICT strategic and operational planning is consistent with the management and direction for ICT investment and assets within the KCG. When performing ICT strategic and operational planning, the KCG ICT department has implemented processes to ensure that ICT goals and objectives are aligned with the KCG departments' business priorities and plans. To this end, the KCG is continuously improving the collection of information related to KCG ICT environment to assist and ensure that informed decision-making can occur and that optimization of ICT resources is encouraged.

4.10.2. The ICT Planning Framework

4.10.2.1 How ICT Planning is aligned

KCG should establish a range of processes and procedures to ensure that the existing and future ICT resources, strategies and plans remain current and up-to-date. The review, assessment and prioritization of KCG ICT strategies and plans should be undertaken annually by a range of interested stakeholder groups.

The ICT department has an integral contributor to the KCG planning framework. The ICT department will implement a consolidated information technology support model and service delivery interfaces to assist ICT management align future planning and decision-making with business requirements.