KNBS
KENYA NATIONAL
BUREAU OF STATISTICS
*Keeping you informed*

# THE KNBS ICT POLICY

DECEMBER 2012

*VISION*

*A centre of excellence in statistics production and management*

*MISSION*

*To effectively manage and coordinate the* entire national statistical system to enhance statistical production and utilization

Herufi House,

Lt. Tumbo lane

P.O. Box 30266 – 00100 GPO

Nairobi, Kenya

Tel: +254-20-317583/86/88,317612/22/23/51

Fax: +254 – 20-315977

Email: info@knbs.or.ke

Web: www.knbs.or.ke

## Preface

Kenya National Bureau of Statistics (KNBS) is the principal agency of the Government for collecting, analysing and disseminating statistical data in Kenya. KNBS is the custodian of official statistical information and is mandated to coordinate all statistical activities, and the National Statistical System (NSS) in the country. To achieve this mandate, KNBS strives to live up to the aspirations of its vision; to be a centre of excellence in statistics production and management.

In order to execute its mandate, the Bureau uses ICT services for enhanced efficiency. In provision of such services, the Bureau commits to ensure that adequate resources are provided to implement a reliable and appropriate IT infrastructure. It is imperative thus that acquisition and usage of such facilities requires to be governed by an organization wide ICT policy.

This policy document strives to provide a framework for providing ICT Services, governance and resources in the Bureau in conformity with the existing government policies, legal and regulatory framework.

Edwin S. Osundwa, EBS
KNBS Board Chairman

## Foreword

Information and Communication Technology (ICT) is a crucial enabler in the achievement of Bureau's Mandate. It is in recognition of this that, the Bureau has formulated this policy to provide guidelines on how ICT services and infrastructure will be availed in the Bureau and provide a framework for the planning, implementation and usage of ICT resources in the Bureau.

In order to execute its mandate, the Bureau relies on ICT services for enhanced efficiency. Thus the Bureau commits to ensure that adequate resources are provided to implement a reliable and appropriate IT infrastructure for guaranteed provision of quality services. An organization wide ICT policy will govern the acquisition and usage of ICT facilities.

I wish to thank the Bureau Management and the ICT Directorate staff for their efforts in developing the comprehensive policy that will guide the development of ICT and its utilization in the Bureau.

Zachary Mwangi

Ag. Director General

## Acronyms

CD – Compact Disk

DICT – Director ICT

DRS –Disaster Recovery Site

DVD – Digital Video Disk

ICT – Information and Communication Technology

ISO – International Organization of Standards

IT – Information Technology

KNBS – Kenya National Bureau of Statistics

LAN – Local Area Network

NSS – National Statistical System

PABX – Private Automatic Branch Exchange

PC – Personal Computers

SAN –Storage Area Network

SLA – Service Level Agreement

WAN – Wide Area Network

# Table of Contents

## 1.0 Introduction

The Kenya National Bureau of Statistics, herein referred to as KNBS or Bureau, became a semi-autonomous body via the Statistics Act 2006 (Kenya Gazette Supplement No. 61 Act No. 4 of 2006).

In order to execute its mandate, the Bureau uses ICT services for enhanced efficiency. In provision of such services, the Bureau commits to ensure that adequate resources are provided to implement a reliable and appropriate IT infrastructure. It is imperative thus that acquisition and usage of such facilities requires to be governed by an organization wide ICT policy.

To address this need, the Bureau has developed this ICT policy in line with the existing government policies, legal and regulatory framework.

## 2.0 The KNBS Mandate

KNBS is mandated by Statistics Act 2006 to carry out the following functions;

a. Act as the principal agency of the government for collecting, analyzing and disseminating statistical data in Kenya
b. The custodian of official statistical information
c. Planning, authorizing, coordinating and supervising all official statistical programs undertaken within the NSS;
d. Establishing standards and promoting the use of best practices and methods in the production and dissemination of statistical information across the NSS.
e. Collecting, compiling, analyzing, abstracting and disseminating statistical information on matters specified in the Act ;
f. Conducting the Population and Housing Census every ten years, and such other censuses and surveys as the Board may determine; and

g. Maintaining a comprehensive and reliable national socio-economic database

## 3.0 Objectives

This policy seeks to;

a. Ensure provision of adequate and reliable information systems in the Bureau
b. provide guidelines on the usage of ICT software, hardware and services in the Bureau
c. ensure information security of Bureau systems and data
d. promote efficient utilization of information systems within the Bureau employees and the National Statistical System(NSS)
e. ensure application of best practices and standards
f. promote spirit of awareness, co-operation, trust and consideration for others.

## 4.0 Scope

This ICT policy covers all IT facilities, hardware, software, and services provided by the Bureau. These are:

a) Facilities
   i. Data processing centre in Nyayo house
   ii. Training room in Herufi house
   iii. Server room(s)
   iv. ICT maintenance room
   v. Data Recovery Site(s) (DRS)
   vi. All ICT facilities installed at KNBS Branches such as Nyayo House, Bima House, County Offices, District offices etc.

b) Services
   i. Provision of guidance and expertise training on ICT

ii. ICT support in software, hardware and any other computing infrastructure
iii. Technical support to KNBS staff and NSS

c) Hardware
i. PCs
ii. Laptops
iii. Printers
iv. Scanners
v. Servers
vi. Network routers and switches
vii. Power backup equipment (eg Uninterruptable Power Backup - UPS)
viii. L.C.D Projectors
ix. Network Devices
x. Cameras (Digital and Camcorders)
xi. PDAs, Smartphones and other Mobile Computing Devices
xii. Diskettes/CDs/DVDs
xiii. Flash-disks/external hard-disks
xiv. PABXs,Telephone heads, fax and photocopiers
xv. All other ICT related hardware

d) Software
i. Network operating systems
ii. PC operating systems
iii. Application software
iv. Utility software
v. Custom made systems

e) County Offices

The policy all covers all county offices and branches. These will be supported from the Bureau headquarters.

f) Gender

The policy caters for persons of all genders without discrimination in line with the national policy on gender.

g) Disability

The policy caters for persons with disabilities in that the Bureau will endeavor to provide specialized equipment and services to disabled persons so as to enable them make maximum use of ICT services.

## 5.0 ICT Facilities Usage

a. All ICT facilities owned by the Bureau will be issued to its staff for official use through the ICT Directorate. The Directorate will be the custodian of ICT systems including software, and hardware as a measure to facilitate standardization. Thus officers will be availed hardware, software and systems relevant to their work requirements.
b. Staff shall take maximum care of such facilities and ensure responsible and secure usage.
c. Sharing of KNBS ICT resources will be encouraged so as to enhance their maximum utilization.
d. Users shall not relocate, repair, reconfigure, modify KNBS ICT equipment or attach external devices other than for data storage to such equipment without the authority from DICT.
e. KNBS shall authorize Staff to use external disks only for the purpose of storing official information. Such external disks must be scanned for viruses and other harmful software.
f. Personal software, hardware or systems shall not be used within KNBS LAN.
g. Food or drinks shall be not allowed on or near any ICT equipment.

## 6.0 ICT Security

a. All KNBS systems and information shall be effectively protected against unauthorized access.
b. The ICT Directorate shall provide network service to staff to transmit data to requesters and store data files in an authenticated central server.
c. Users within same directorate/working group will be given access level that allows them access to their files/folders.
d. For traceability and identification, all hardware shall be bar-coded and included in the KNBS asset register. This shall include any hardware bought for /donated to KNBS by external agencies.
e. ICT devices are susceptible to theft and unauthorized access, thus, strong security measure to safeguard them shall be provided.
f. Portable or laptop computers shall not be left unattended in public places, and shall be carried as hand luggage for security.
g. Portable computing equipment for short term lending shall be stored in secure lockable cabinets.
h. An updated register of all ICT equipment e.g. LCD projectors loaned out to authorized personnel shall be maintained.
i. All data storage media shall be stored in secure environments that meet manufacturer's specifications for temperature and humidity.
j. Hard copies of systems documentation shall be physically secured in filing cabinets when not in use.
k. It is the responsibility of respective users of any non LAN-connected and official computing equipment (especially laptops/notebooks) to arrange with the ICT support for

installation of antivirus software and to perform periodic (at most every fortnight) updates to the antivirus.

l. All ICT hardware or software will not be taken off-site from KNBS offices, for serving and /or upgrading without written authority from DICT.

## 7.0 Network Access & Permissions

a. Each user will have only one personal identification code (User ID/user name and password) with necessary access levels and privileges.
b. User IDs will be consistent in structure i.e. the fist letter of the first name and last name, all in lower cases (ignoring middle names). If this combination conflicts with another user, then the first letter of second name will be used as the second letter of the user ID. If the officer does not have other names, then letter 'a' through 'z' will be used so that user ID is unique within KNBS access systems.
c. All devices will require access credentials (user ID and password) to be accessed over the network. Guidelines on structure of user IDs and passwords will be provided by ICT Directorate.
d. Users will be responsible for the confidentiality of their access credentials and prevention of any unauthorized access to ICT equipment. Any attempt to use other users' credentials to gain access to network resources is strictly disallowed. Any account found to be compromised or shared shall be discontinued and a new one issued where necessary.
e. Only authorized personnel are allowed access to ICT resources.
f. Access credentials shall immediately be deactivated and confirmed in a clearance certificate by the DICT once a member of staff ceases to be an employee of the Bureau.

g. DICT is authorized to gain access to a user account and folders if that account is suspected to have breached systems security or is in violation of this policy.
h. The ICT Directorate shall enforce standardization of systems and network configuration, including directory structures, to simplify network management.

## 8.0 Website(s)

a. The Bureau shall ensure that the KNBS Website(s) is kept in an updated status at all times. By use of the latest technology, the website shall be maintained in a user friendly and accessible state.
b. All requests for changes on the website shall be subject to the approval of the KNBS ICT committee that shall comprise of representatives of the Bureau directorates and chaired by the DICT.
c. The ICT Directorate shall ensure that the website is always available to the public.

## 9.0 ICT Equipment Maintenance.

a. The DICT shall ensure that all ICT equipment is kept in proper working condition at all times.
b. All ICT equipment shall be maintained in accordance with the procedure for ICT equipment maintenance.
c. In areas where the Bureau has no adequate internal capacity, annual maintenance contracts will be entered into with service providers.

## 10.0 Email Usage

a. Staff shall be issued with official standardized e-mail addresses as outlined in section 8.0 above.
b. All official email communications shall be through official email addresses. DICT will ensure that mail service is available to staff always.
c. The KNBS's Intranet will be used to communicate all relatively static information (e.g. policies, procedures, briefing documents, reference material and other standing information).
d. Email users shall avoid broadcast communication (i.e. send to large groups of people using email aliases) unless where absolutely necessary. One must always ensure proper audience segregation is used before sending an email.
e. KNBS mail service shall not be used to broadcast other unofficial information or requests (e.g. information or opinions on political matters, social matters, and personal requests for information etc.)
f. Emails with attachments greater than 2MB will require authorization from DICT. This will remove unnecessary load on the network and the mail server so as to guarantee equitable bandwidth sharing by all staff.

## 11.0 Internal ICT Support

a. While KNBS will strive to provide ICT support services, officers assigned to hardware must ensure they are not exposed to risks that can cause their damage.
b. ICT officers will be available to offer technical support on any software or hardware upon users' requests.

c. Where applicable, equipment to be used out of office shall be accompanied by an ICT Technician to ensure proper packaging, offloading and installation at destination.

## **12.0** The Internet

a. All connections to the Internet within KNBS offices shall be implemented through the KNBS Internet connections via a firewall.
b. To protect KNBS systems from Internet attacks or denial of service by Internet malware, all software downloads shall be authorized by DICT. Such a download will be passed on to the requester only if it passes the ICT security tests and if it is permitted for free use by its manufacturers.
c. No copyright material shall be downloaded from the internet or utilized in breach of its license agreement.
d. Internet services shall be provided only through the KNBS Internet connection or KNBS USB modems or any other approved gadgets.
e. To optimize internet bandwidth usage, Bureau's network shall not be used to stream music and video as these lead to deprivation of the same capacity to legitimate users during normal working hours except, where such permission is granted by DICT in writing.
f. KNBS internet and network resources shall not be used to access or transfer any material containing:
    i. Derogatory remarks based on race, religion, gender, physical disability or sexual preference.
    ii. Images or references that may be considered to be offensive or in breach of any law or regulation.

## 13.0 Out-Sourced ICT services

a. The Bureau shall out-source ICT Equipment and/or services whenever such capacity lacks in the Bureau with approval from the Director General upon recommendation from DICT. Such a need shall be supported by a needs assessment report from DICT.
b. Acquisition of such services will be guided by the Public Procurement and Disposal Act (PPDA),2005, and Public Procurement and Disposal Regulations (PPDR), 2006.
c. All out-sourced ICT equipment and services will be supervised by DICT in accordance with Service Level Agreements (SLAs) that are signed in consultation with DICT.
d. The out-sourced services shall be based on annual contracts that may be renewed based on recommendations from the ICT directorate.

## 14.0 ICT Staffing

a. The Bureau commits to equip and maintain adequate and highly skilled ICT personnel for guaranteed minimum acceptable ICT service level.
b. The ICT function will be executed through the ICT Directorate headed by a Director.

## 15.0 Acquisition and Disposal of ICT Facilities

a) Acquisition of ICT Facilities
   i. Acquisition of ICT facilities shall be guided by the Public Procurement Procedures and Guidelines in the Public Procurement and Disposal Act (PPDA), 2005, Public Procurement and Disposal Regulations(PPDR)2006, Best Practices and the KNBS Procurement Manual. Where funds are donated from external sources, the respective donor

conditionalities, terms, agreements or memoranda of understanding shall apply.

ii. All User requests for acquisition of items of ICT nature shall be channeled through the DICT who will confirm lack or availability of such items in the Bureau. If not available, DICT will prepare specifications in consultation with the requesting Directorate and forward the request to the Director General for approval.

iii. In order to minimize the costs, KNBS will standardize software and hardware to be used within the Bureau with advice from DICT. This will be reviewed annually as need arises.

iv. All Directors will forward to DICT their software and /or systems needs who will offer technical guidance and support in facilitating the acquisition process.

v. ICT goods, related services and/or works once acquired will be received by the Bureau's Inspection and Acceptance Committee in line with The Public Procurement and Disposal Act (PPDA), 2005 and Public Procurement and Disposal Regulations (PPDR), 2006 framework. The Committee shall seek professional assistance from DICT.

vi. The ICT Directorate shall ensure that all software licenses in use in the Bureau are promptly renewed to guarantee smooth Bureau operations and continuous software updates and support from manufacturers.

vii. The Bureau will strive to maintain reliable hardware infrastructure by upgrading aging ICT equipment every three years.

viii. In order to avail adequate and reliable computing capacity to the technical staff, the Bureau shall provide at least one functional computer to every technical staff both at the headquarters and at the branches.

b) Disposal

i. DICT shall identify hardware and software to be disposed and liaise with Procurement Department for assessment leading to disposal as per PPDA, 2005 and the PPDR, 2006.

ii. DICT shall ensure that all equipment earmarked for disposal are cleared of Bureau data and storage media destroyed.

## **16.0** Backup & Disaster Recovery

a. KNBS' information resources such as data, business contacts, emails, text documents, presentations, contracts, accounts and other valuable information shall be safely preserved in a recoverable state.

b. ICT Directorate will maintain consistent automated backup mechanisms to preserve KNBS data in a distributed Storage Area Network (SAN) and at a DRS in order to ensure data recovery in the event of accidental loss.

c. All KNBS data shall be saved in organized shared folders in allocated branch servers from where they will be backed up in SAN and Disaster Recovery Site (DRS) through synchronized mechanism in addition to tapes or external drives in accordance with the KNBS Backup Plan.

d. Network and server administrators will ensure data is copied to these allocated servers and in all other backup destinations.

e. It is the responsibility of the respective users of any non LAN-connected computing equipment (including laptops/notebooks) to arrange with the server administrator for the transfer of official data from these non LAN-connected equipment to the relevant server folders every day where practical.

f. Any unofficial files shall not be allowed on KNBS Servers.

g. Only authorized personnel will be able to visit off-site DRS.

h. To implement an ICT seamless backup service, all officers connected to KNBS LAN shall login to centralized authentication servers. Officers working from remote locations will be required to dock to the KNBS network to back up official data.

## 17.0 Printers, Telephone Lines, Fax, Scanners and Copiers

a. KNBS Staff are expected to use the above peripheral devices responsibly. Irresponsible or usage of these facilities for personal gain is prohibited, and may lead to denial of the service and/or surcharge.
b. Where possible, users are required to print on both sides of the paper. ICT support team will give guidance on how various printers are able to print both sides.
c. Printers will be configured to be shared by many users and placed in secured open offices where possible.
d. Unofficial calls and fax will be charged on the user.
e. An electronic document scanner shall be used to minimize usage of fax machines, printers and copiers, saved in suitable formats and emailed to recipients.

## 18.0 ICT Training

a. Bureau's ICT training needs shall be assessed by the ICT Directorate and recommendations captured in the Bureau's training plan.
b. The DICT shall recommend ICT trainings relevant for every section and forward requirements to Director Finance and Administration.
c. KNBS staff will be trained on emerging technologies as the Bureau may determine from time to time in consultation with DICT.

## **19.0** Online Subscriptions for KNBS products

a. Online subscriptions for KNBS statistical products shall be done via the KNBS web portal. Such subscription shall be handled by DICT as per the Bureau's Data Access and Dissemination Policy.
b. Official payments to such online subscriptions shall follow the Finance Manual.

## **20.0** Enforcement and Control

a. Deliberate breach of this policy statement may lead to disciplinary measures in accordance with KNBS Human Resource Manual. These may include but not limited to the offender being denied access to computing facilities or surcharge for the loss or abuse of ICT facility or service.
b. Whenever surcharge is imposed on negligence as noted in (a) above, due process will be followed in imposing the surcharge.
c. Unauthorized access to information, facility or computer (including workstations and PCs), over network or to modify its contents is strictly forbidden.
d. Officers within KNBS network shall not write, publish, browse, bookmark, access or download obscene, pornographic or pedophilia materials.
e. All hardware, software and /or systems in use in KNBS stations shall be licensed. Any officer using unlicensed products shall bear legal consequences for the product as per 'the Copyright Act, 2001'.

## 21.0 Privacy and Confidentiality

a. The Bureau shall guarantee right to privacy and confidentiality of individual staff information while discharging ICT services.
b. Information/services/resources available within IT facilities will not be used to monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Without limitation to this provision, the following shall be excluded:
    i. In the case of a specific allegation of misconduct or for any other investigation purpose, the Director General may authorize access to such information or denial of service while the staff is under investigation.
    ii. Where the ICT Directorate or any other Bureau section cannot avoid accessing such information whilst administering, resolving ICT systems problems or in their day to day work activities.

## 22.0 Revision

This policy shall be revised every three years or as and when need arises under the authority of the Director General to keep in tandem with changes in technology, statutory regulations or for any other purposes as may be advised from time to time by DICT.

References:


i. National Policy on Information and Communication Technology (ICT); GoK, 2007.

ii. ICT Standards and Guidelines. Directorate Of E-Government. Kenya (2011)

iii. ICT Policy Formulation and E-Strategy Development. A Comprehensive Guidebook. Asia-Pacific Development information Programme , UNDP,2011.