THE NAIROBI CITY COUNTY ASSEMBLY
ICT POLICY

MARCH2016

Acronyms

CD – Compact Disk

DRS –Disaster Recovery Site

DVD – Digital Video Disk

ICT – Information and Communication Technology

ISO – International Organization of Standards

IT – Information Technology

NCCA – Nairobi City County Assembly

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

1.0 Introduction

The Nairobi City County Assembly, herein referred to as NCCA or Assembly, has the following mandate;

I. Oversight
II. Representation
III. Legislation

In order to execute its mandate, the Assembly uses ICT services for enhanced efficiency. In provision of such services, the Assembly 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 Assembly has developed this ICT policy in line with the existing government policies, legal and regulatory framework.

2.0 Objectives

This policy seeks to;

i. Ensure provision of adequate and reliable information systems in the Assembly
ii. provide guidelines on the usage of ICT software, hardware and services in the Assembly
iii. Ensure information security of Assembly systems and data
iv. Promote efficient utilization of information systems within the Assembly employees
v. Ensure application of best practices and standards
vi. Promote spirit of awareness, co-operation, trust and consideration for others.

3.0 Scope

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

a) Facilities

i. County Assembly Offices
ii. Committee rooms
iii. Server room(s)
iv. ICT maintenance room
v. CCTV Control room

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 NCCA staff and MCAs

c) Hardware

i. PCs
ii. Laptops
iii. Printers
iv. Scanners
v. Servers
vi. Network routers and switches
vii. Power backup equipment (e.g. 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

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 Assembly will endeavor to provide specialized equipment and services to disabled persons so as to enable them make maximum use of ICT services.

4.0 ICT Facilities Usage

i. All ICT facilities owned by the Assembly will be issued to its staff for official use through the ICT Section. The Section 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.
ii. Staff shall take maximum care of such facilities and ensure responsible and secure usage.
iii. Sharing of NCCA ICT resources will be encouraged so as to enhance their maximum utilization.
iv. Users shall not relocate, repair, reconfigure, modify NCCA ICT equipment or attach external devices other than for data storage to such equipment without the authority from ICT Officer.
v. NCCA 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.

vi. Personal software, hardware or systems shall not be used within NCCA LAN.

vii. Food or drinks shall be not allowed on or near any ICT Equipment.

5.0 ICT Security

i. All NCCA systems and information shall be effectively protected against unauthorized access.

ii. The ICT Section shall provide network service to staff to transmit data to requesters and store data files in an authenticated central server.

iii. Users within same Department/Section/working group will be given access level that allows them access to their files/folders.

iv. For traceability and identification, all hardware shall be bar-coded and included in the NCCA asset register. This shall include any hardware bought for /donated to NCCA by external agencies.

v. ICT devices are susceptible to theft and unauthorized access, thus, strong security measure to safeguard them shall be provided.

vi. Portable or laptop computers shall not be left unattended in public places, and shall be carried as hand luggage for security.

vii. Portable computing equipment for short term lending shall be stored in secure lockable cabinets.

viii. An updated register of all ICT equipment e.g. LCD projectors loaned out to authorized personnel shall be maintained.

ix. All data storage media shall be stored in secure environments that meet manufacturer's specifications for temperature and humidity.

x. Hard copies of systems documentation shall be physically secured in filing cabinets when not in use.

xi. 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.

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

6.0 Network Access & Permissions

i. Each user will have only one personal identification code (User ID/user name and password) with necessary access levels and privileges.

ii. User IDs will be consistent in structure i.e. the first name and last name, all in lower cases (ignoring middle names). If the Officer does not have other names, then letter 'a' through 'z' will be used so that user ID is unique within NCCA access systems.

iii. 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 Section.

iv. 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.

v. Only authorized personnel are allowed access to ICT resources.

vi. Access credentials shall immediately be deactivated and confirmed in a clearance certificate by the ICT Officer once a member of staff ceases to be an employee of the Assembly.

vii. ICT Officer 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.

viii. The ICT Section shall enforce standardization of systems and network configuration, including directory structures, to simplify network management.

7.0 Website(s)

i. The Assembly shall ensure that the NCCA 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.

ii. All requests for changes on the website shall be subject to the approval of the NCCA Clerk.

iii. The ICT Section shall ensure that the website is always available to the public.

8.0 ICT Equipment Maintenance.

i. The ICT Officer shall ensure that all ICT equipment is kept in proper working condition at all times.

ii. All ICT equipment shall be maintained in accordance with the procedure for ICT equipment maintenance.

iii. In areas where the Assembly has no adequate internal capacity, annual maintenance contracts will be entered into with service providers.

9.0 Email Usage

i. Staff shall be issued with official standardized e-mail addresses.

ii. All official email communications shall be through official email addresses. ICT Officer will ensure that mail service is available to staff always.

iii. The NCCA's Intranet will be used to communicate all relatively static information (e.g. policies, procedures, briefing documents, reference material and other standing information).

iv. 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.

v. NCCA 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.)

vi. Emails with attachments greater than 2MB will require authorization from ICT Officer. This will remove unnecessary load on the network and the mail server so as to guarantee equitable bandwidth sharing by all staff.

10.0 Internal ICT Support

i. While NCCA will strive to provide ICT support services, Officers assigned to hardware must ensure they are not exposed to risks that can cause their damage.

ii. ICT Officers will be available to offer technical support on any software or hardware upon users' requests.

iii. 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.

11.0 The Internet

i. All connections to the Internet within NCCA offices shall be implemented through the NCCA Internet connections via a firewall.

ii. To protect NCCA systems from Internet attacks or denial of service by Internet malware, all software downloads shall be authorized by ICT Officer. 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.

iii. No copyright material shall be downloaded from the internet or utilized in breach of its license agreement.

iv. Internet services shall be provided only through the NCCA Internet connection or NCCA USB modems or any other approved gadgets.

v. To optimize internet bandwidth usage, Assembly'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 ICT Officer in writing.

vi. NCCA internet and network resources shall not be used to access or transfer any material containing:

a. Derogatory remarks based on race, religion, gender, physical disability or sexual preference.

b. Images or references that may be considered to be offensive or in breach of any law or regulation.

12.0 Out-Sourced ICT services

i. The Assembly shall out-source ICT Equipment and/or services whenever such capacity lacks in the Assembly with approval from the County Assembly Clerk upon recommendation from ICT Officer. Such a need shall be supported by a needs assessment report from ICT Officer.

ii. Acquisition of such services will be guided by the Public Procurement and Disposal Act (PPDA), 2015, and Public Procurement and Disposal Regulations (PPDR), 2006.

iii. All out-sourced ICT equipment and services will be supervised by ICT Officer in accordance with Service Level Agreements (SLAs) that are signed in consultation with County Assembly Clerk.

iv. The out-sourced services shall be based on annual contracts that may be renewed based on recommendations from the ICT Section.

13.0 ICT Staffing

i. The Assembly commits to equip and maintain adequate and highly skilled ICT personnel for guaranteed minimum acceptable ICT service level.

ii. The ICT function will be executed through the ICT Section headed by an ICT Officer.

14.0 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), 2015, Public Procurement and Disposal Regulations(PPDR)2006, Best Practices and the NCCA Procurement Manual. Where funds are donated from external sources, the respective donor Conditionality's, terms, agreements or memoranda of understanding shall apply.

ii. All User requests for acquisition of items of ICT nature shall be channeled through the ICT Officer who will confirm lack or availability of such items in the Assembly. If not available, ICT Officer will prepare specifications in consultation with the requesting Section and forward the request to the County Assembly Clerk for approval.

iii. In order to minimize the costs, NCCA will standardize software and hardware to be used within the Assembly with advice from ICT Officer. This will be reviewed annually as need arises.

iv. All Heads of Departments will forward to ICT Officer 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 Assembly's Inspection and Acceptance Committee in line with The Public Procurement and Disposal Act (PPDA), 2015 and Public Procurement and Disposal Regulations (PPDR), 2006 framework. The Committee shall seek professional assistance from ICT Officer.

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

vii. The Assembly 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 Assembly shall provide at least one functional computer to every technical staff.

b) Disposal

i. ICT Officer shall identify hardware and software to be disposed and liaise with Procurement Department for assessment leading to disposal as per PPDA, 2015 and the PPDR, 2006.

ii. ICT Officer shall ensure that all equipment earmarked for disposal is cleared of Assembly data and storage media destroyed.

15.0 Backup & Disaster Recovery

i. NCCA' 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.

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

iii. All NCCA 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 NCCA Backup Plan.

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

v. 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.

vi. Any unofficial files shall not be allowed on NCCA Servers.

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

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

16.0 Printers, Telephone Lines, Fax, Scanners and Copiers

i. NCCA 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.

ii. 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.

iii. Printers will be configured to be shared by many users and placed in secured open offices where possible.

iv. Unofficial calls and fax will be charged on the user.

v. An electronic document scanner shall be used to minimize usage of fax machines, printers and copiers, saved in suitable formats and emailed to recipients.

17.0 ICT Training

i. Assembly's ICT training needs shall be assessed by the ICT Section and recommendations captured in the Assembly's training plan.

ii. The ICT Officer shall recommend ICT trainings relevant for every section and forward requirements to Director Finance and Administration.

iii. NCCA staff will be trained on emerging technologies as the Assembly may determine from time to time in consultation with ICT Officer.

18.0 Enforcement and Control

i. Deliberate breach of this policy statement may lead to disciplinary measures in accordance with NCCA 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.

ii. Whenever surcharge is imposed on negligence as noted in (i) above, due process will be followed in imposing the surcharge.

iii. Unauthorized access to information, facility or computer (including workstations and PCs), over network or to modify its contents is strictly forbidden.

iv. Officers within NCCA network shall not write, publish, browse, bookmark, access or download obscene, pornographic or pedophilia materials.

v. All hardware, software and /or systems in use in NCCA stations shall be licensed. Any Officer using unlicensed products shall bear legal consequences for the product as per 'the Copyright Act, 2001'.

19.0 Privacy and Confidentiality

i. The Assembly shall guarantee right to privacy and confidentiality of individual staff information while discharging ICT services.

ii. 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:

a) In the case of a specific allegation of misconduct or for any other investigation purpose, the County Assembly Clerk may authorize access to such information or denial of service while the staff is under investigation.

b) Where the ICT Section or any other Assembly 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 County Assembly Clerk to keep in tandem with changes in technology, statutory regulations or for any other purposes as may be advised from time to time by ICT Officer.

References:

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

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

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