# NATIONAL LAND COMMISSION

# INFORMATION COMMUNICATION TECHNOLOGY

# ICT POLICY

**DOCUMENT REVISION HISTORY**

| Version | Date | Author(s) | Revision Notes |
|---|---|---|---|
| 1.0 | August 2015 | ICT Department | Initial draft |
| 1.1 | | | |
| 1.2 | | | |
| 1.3 | | | |
| 1.4 | | | |
| 1.5 | | | |
| 1.6 | | | |
| 1.7 | | | |

# Table of Contents

## FOREWORD

In accordance with its broader strategic objectives, The National Land Commission has procured and implemented at various locations, Information and Communication Technologies (ICTs) that are used to create, process, store, share and disseminate data and information. These assets represent a significant economic investment by the Commission. The data and information resources they create, store and disseminate could be priceless and irreplaceable.

Their continued availability in furtherance of the NLC core business is of paramount importance, hence, there is a compelling need to secure and control access to them.

Users of the NLC information systems and other stakeholders have an expectation of privacy for their personal data gathered by the Commission in the normal course of it's duty. Therefore, there is a reasonable expectation from users that the Commission would institute controls to conserve the privacy of personal information.

Confidentiality of information is demanded by the government regulations and conventions. Since the Commission operates as an independent government institution dealing with land matters, misuse of the institution's ICT assets could tarnish its goodwill and reputation.

The Commission acknowledges that there is a well-founded requirement to maintain the integrity and confidentiality of its electronic data and information. Such assets must be protected from unauthorized access and intrusions, malicious misuse, inadvertent compromise and intentional damage or destruction. Accordingly, the Commission is obliged to ensure that appropriate security measures are enacted for all electronic data and information, as well as ICT equipment and processes in its domain of ownership and control.

Tom Aziz Chavangi
CEO/ SECRETARY.

## ACKNOWLEDGEMENT

We wish to acknowledge the tireless effort put by the NLC ICT team in coming up with this policy document as well as the Directors, the CEO, Commissioners and the entire commission's staff who took their time to review, critic and amend this ICT Policy.

The following are ICT Team members who were involved in coming up with this ICT Policy;

| | | |
|---|---|---|
| 1 | Amos Kasaine | Head Of ICT |
| 2 | Julius Tarus | Chief Systems Administrator |
| 3 | Meshack Mwiti | Chief Network Administrator |
| 4 | Caroline Kimisik | Senior Systems Administrator |
| 5 | Augustine Orwa | System Administrator |
| 6 | Raphael Masindet | ICT officer |
| 7 | Nelly Mundati | ICT officer |
| 8 | Micheal Mathenge | ICT officer |
| 9 | Edwin Okello | Clerical Officer |
| 10 | Boniface Ketora | Clerical Officer |

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **CD-ROM** | Compact Disc Read only Memory |
| **NLC** | National Land Commission |
| **DTUs** | Data Terminal Unit |
| **DVD** | Digital Versatile Disc |
| **DHCP** | Dynamic Host Configuration Protocol |
| **GOK** | Government of Kenya |
| **HOD** | Head of Department |
| **HRM** | Human Resource Management |
| **ICT** | Information and communication Technology |
| **ISO** | International Standards Organization |
| **LAN** | Local Area Network |
| **PDA** | Personal Digital Assistant |
| **SCMD** | Supply Chain Management Department |
| **SLA** | Service Level Agreements |
| **TOT** | Training of Trainers |
| **UPS** | Uninterruptible power supply |
| **VLANs** | Virtual Local Area Networks |
| **VPNs** | Virtual Private Networks |
| **WAN** | Wide Area Network |
| **MPLS** | Multi-Protocol Label Switching |
| **NLIMS** | National Land Information Management System |

## INTRODUCTION

Information and Communication Technology (ICT) has become the backbone of day to day operations in all organizations. The National Land Commission (NLC) is not an exception. While the management of NLC recognizes this fact, organizations all over the world, including NLC, are faced with the challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance.

This document therefore aims to assist the management of National Land Commission (NLC) in the management of Information Technology within the Commission. Information Technology is a very dynamic sector and new technologies are being developed every minute of everyday life. It is therefore imperative the Commission develops the ICT policy to help in managing Information Technology trends, the policy should focus on the mandate and the strategic Plan of the Commission.

The Commission is deliberately undertaking service transformation through the use of ICT to effectively and efficiently serve its customers who mainly include its employees and members of the public seeking services. In order to provide transparent, efficient and accountable systems, the Commission has invested heavily in providing tools required to perform these functions. This has been achieved by providing the staff with access to electronic equipment and services such as computers, email, Internet and business support systems. Further, the NLC is undertaking training of its staff in ICT to equip them with relevant skills to be able to handle ICT related functions.

Due to the fact that the NLC handles sensitive and critical information, there is need for caution to be exercised while undertaking government businesses in order to maintain integrity and confidentiality of the information.

This document is set out to provide guidelines and procedures to NLC members of staff and third parties on matters related to ICT use, and also to ensure compliance to the same.

# NATIONAL LAND COMMISSION

## MANDATE

The mandate of the National Land Commission (NLC) is drawn from the National Land Policy of 2009, Constitution of Kenya 2010, National Land Commission Act, 2012, the Land Act 2012 and the Land Registration Act of 2012.

## CORE FUNCTIONS

The core functions of the Commission are:

I. To manage public land on behalf of the National and County Governments;
II. To recommend a National land policy to the National Government;
III. To advise the national government on a comprehensive programme for the registration of title in land throughout Kenya;
IV. To conduct research related to land and the use of natural resources, and make recommendations to appropriate authorities;
V. To initiate investigations, on its own initiative .or on a complaint, into present or historical land injustices, and recommend appropriate redress;
VI. To encourage the application of traditional dispute resolution mechanisms in land conflicts;
VII. To assess tax on land and premiums on immovable property in any area designated by law;
VIII. To monitor and have oversight responsibilities over land use planning throughout the country.

## VISION

"Excellent administration and management of land for sustainable development"

## MISSION

"To facilitate sustainable land use in Kenya through a holistic land policy, efficient land management practices, equitable access to land, comprehensive land registration and applying appropriate land dispute handling mechanism".

### CORE VALUES

The Commission's corporate culture is based on its core values which include:-

i) Efficiency
ii) Team work
iii) Transparency and accountability
iv) Innovativeness
v) Zero tolerance to corruption
vi) Integrity
vii) Professionalism

### ICT DEPARTMENT

The ICT Department which is based at the NLC headquarters is responsible for all matters pertaining to ICT such as coordinating, supervising, quality control, training, user support, development and management of the NLC website, automation of business processes, and provision of technical advice on ICT issue. The Department also ensures that all the ICT equipment are in good working condition, spearhead actualization of innovations that need automation, design and develop systems, implementation of security measures and management of the Commission's network infrastructure.

For this to be achieved there needs to be an ICT policy in place. This policy aims at providing the framework for developing and maintaining an effective Information Communication Technology environment.

### VISION

To use ICT as a dynamic tool of choice in provision of data and information services.

### MISSION

Provide effective and efficient ICT infrastructure and secure information technology systems that support timely access to information.

## OBJECTIVES OF THE POLICY

It is expected that this policy will help NLC re-engineer its processes with a view of efficient and effective delivery of data and information services. Specific objectives of the policy include:

1. Ensure provision of adequate and reliable information system in the Commission

2. Provide guidelines on the usage of ICT software and services in the Commission systems and data.
3. Promote efficient utilization of information system within the commission and NLIMS systems.
4. Ensure application of best practices and standards.

# CHAPTER 1 POLICY OVERVIEW

## 1.1 The Policy Overview

All ICT equipment, system, data, software and staff at the NLC are governed by this ICT Policy. All members of staff of the NLC shall adhere to this policy.

Specifically, the purpose of the policy is to:-

- Establish standardized guidelines for the use of government's computing resources collectively termed as Information and Communications Technology at the Commission.
- Protect the NLC ICT assets ie the infrastructure, data and business processes.
- Provide guidelines on acquisition, use and disposal of ICT equipment.
- Provide guidelines on design, installation and continuous management of ICT services.
- Outline the role of the ICT department in terms of supervision and coordination of ICT activities in the Commission.

By adopting the policy comprehensively, all users will help ensure ICT resources are used:

- Legally
- Securely
- Cost effectively
- Without undermining the Commission and the government of Kenya
- In the spirit of co-operation, trust and consideration for others.

## 1.2 Policy document approval, distribution and enforcement

This document has been approved by the CEO/ Secretary and distributed to all Directorates and Heads of Departments. The HODs shall in turn ensure that all users read, understand and adhere to this policy. The document has been distributed both in soft and hard copies. The ICT Department is mandated to coordinate the implementation of this policy.

### 1.3 Accessibility

It is intended that this ICT Policy is accessible in its entirety at Departmental and Section Heads' Offices, NLC intranets, ICT Department and the library. An abridged version will be accessible publicly via the NLC website (www.nlc.or.ke).

### 1.4 Policy revision

The document will be reviewed annually based on the following factors:-

1) The policy is deemed to be a dynamic document that will be revised as required to deal with changes in technology, applications, procedures, legal requirements, social imperatives, and perceived threats.
2) The policy shall be revised subject to changes in Government policy and structure.

### 1.5 Applicability

This policy shall apply to:-

1) **Commission staff:** It is the responsibility of all Directorates/ Departmental Heads to ensure that this policy is clearly communicated, understood and adhered to.
2) **External service providers:** Contractors, vendors and suppliers providing services to the Commission especially dealing with ICT infrastructure, software and all intellectual property and other data stored on systems within the Commission.

### 1.6 Scope of policy

This policy has been developed for use by the National Land Commission. The scope of this policy focuses on staff, vendors and third parties; and ICT resources including hardware, software, licensing, maintenance, warranty, intellectual property rights, training, standardization and acquisition. It will also address the role of the ICT Department.

The NLC has made a substantial investment in ICT resources in order to facilitate efficient service delivery. This policy therefore is established in order to:

- Protect the NLC ICT assets and investments
- Safeguard the information contained within the NLC systems
- Reduce business and legal risk
- Protect the reputation of the Commission
- Ensure the systems' integrity, confidentiality and availability

All users are therefore expected to familiarize themselves with the laid down guidelines in this policy. This document also provides information for all computer and system users about security and informs them of the risks associated with security violations.

## 1.7 User ethics

The confidentiality of information is mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degree of confidentiality. The hardware and software components that constitute the NLC ICT assets represent a sizable monetary investment that must be protected. The same is applicable for the data and information stored in its IT systems, some of which have taken huge resources to generate, and most of which can never be reproduced.

The use of ICT assets in a manner other than the intended purpose poses a danger to the NLC reputation or a violation of the law. This may lead to disciplinary action and where applicable prosecution.

Proper functionality of IT systems is required for the efficient operation of the NLC core business. As the custodian of NLC data, staff members are expected to handle the electronic information with utmost care and confidentiality. Any misuse such as deletions or amendments without authority from the relevant persons will be treated as an offence.

In the spirit of this policy, all staff members shall share ICT resources at the Commission. These resources are provided to staff for the purpose of conducting NLC core business. However, these facilities must be used responsibly by everyone. Misuse of these resources has the potential to negatively impact productivity, interfere with the work or rights of others, erodes public confidence and may attract legal redress. Any action that may lead to exposure of Commission data, unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

Users of Commission ICT resources are required to comply with all regulations referred to in this document. Users shall agree to refrain from engaging in any activity that would subject the Commission to any liability. The NLC reserves the right to amend this policy at any time without prior notice and to take such further actions as may be necessary or appropriate.

In order to protect the integrity of Commission ICT assets and its users against unauthorized or improper use and to investigate possible violation of Commission rules and policies, measures shall be put in place.

The NLC reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove or otherwise alter any data, file or system resource which may undermine the authorized use of any computing facility or which is used in violation of NLC rules or policies.

The NLC also reserves the right to periodically examine any system and other usage and disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

## 1.8 Responsibilities

General responsibilities pertaining to this policy by various players are set forth in this section.

### 1.8.1 CEO/ Secretary

Shall provide overall leadership in the adoption and implementation of the policy

### 1.8.2 Directorate/ Departmental Heads

Shall facilitate the implementation of the policy within their departments.

### 1.8.3 The ICT Head

1) In liaison with Heads of Directorates/ Departments, the ICT Department shall ensure that all users are aware of and comply with the policy.
2) Shall create appropriate and up to date performance standards, control practices, and procedures designed to provide reasonable assurance that all staff observe this policy.
3) Shall ensure that ICT resources supplied meet or exceed the minimum requirements.

### 1.8.4 The staff

1) Shall safeguard the ICT equipment in their custody.
2) Shall be responsible for protection and preservation of the NLC data.
3) Shall not take any ICT equipment belonging to the NLC without a written informed consent of the respective Directorate/ Department Head. Written informed consent means that the Directorate/ Department head has authorized in form of signing out/in the movement of, and purpose of movement.

4) Shall ensure that removable storage devices are kept out of sight when not in use and if they contain sensitive or confidential data they should be locked up.
5) Shall ensure that ICT equipment are kept away from environmental hazardous conditions such as direct sunlight ,magnetic fields, smoke, liquids, and extreme heat
6) Shall make requests for ICT resources through the ICT Department for technical advice and concurrence.

### 1.8.5 ICT Department Staff

The ICT Department staff shall;

1) Be responsible for all equipment installation, disconnection, modification, and relocation, with authorization of the ICT Head. This does not apply to temporary movement of portable computers for which an initial connection has been set by ICT.
2) Develop and maintain written standards and procedures necessary to ensure implementation and compliance with the policy.
3) Provide appropriate support and guidance to assist users fulfill their responsibilities under this policy.
4) Be responsible for creation, deletion, enabling, disabling of accounts and resetting of passwords.
5) Ensure that the computer systems are available to all users at optimal levels.

# CHAPTER 2 ICT USE

## 2.1 ICT RESOURCE USE POLICY

### 2.1.1 Purpose

To ensure efficient and appropriate use of ICT resources.

### 2.1.2 Scope

The scope of this policy applies to all staff and third parties accessing or utilizing the Commission's ICT resources and specifies authorized and unauthorized use. The ICT resources can either be owned or leased by the NLC and include the following:-

i) All computer-related equipment, including desktop personal computers, terminals, workstations, PDAs, projectors, scanners, cameras, wireless computing devices, telecomm equipment, networks, printers, servers and shared network resources, specialized equipment and all peripherals.

ii) All electronic communications equipment, including telephones, , fax machines, mobile phones, hand-held devices, IP phones, wired or wireless communications devices and services, internet, intranet, e-mail and other on-line services.

iii) All software including off-the-shelf, licensed business software applications, in house developed applications, vendor/supplier customized applications, operating systems, databases, firmware, and any other software.

iv) All intellectual property and other data stored in NLC equipment.

### 2.1.3 Policy

i) Commission ICT resources shall be used for Commission's authorized activities only.

ii) All staff shall ensure efficient and appropriate use that guarantees that ICT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

iii) The use of Commission ICT resources for unauthorized activities is against NLC policy and violators will be penalized.

### 2.1.4 Guidelines

- Staff shall not use ICT resources at their disposal to hurt or harm others through improper use.

- The use of NLC ICT resources by any non-NLC users must be approved in writing by the ICT Head.
- ICT resources shall be moved after obtaining written authorization from ICT Head.

## 2.2 ACQUISITION OF ICT RESOURCES POLICY

### 2.2.1 Purpose

To provide a guideline on acquisition and ownership of ICT resources.

### 2.2.2 Scope

This policy applies to all ICT resources acquired through procurement or under MOUs/grants/donations/agreements/gifts and the resulting ownership transferred to the Commission.

### 2.2.3 Policy

- All ICT resources acquired by the NLC belong to and shall remain the property of the Commission.
- All ICT resources acquired by the NLC under Grants/MOU/Agreements/Donation must have elaborate terms and conditions which include and specify ownership.
- ICT Department shall facilitate provision of technical specifications for the acquisition of ICT resources.

### 2.2.4 Guidelines

- All requisitions for procurement of hardware, software and specialized equipment shall be channeled through the ICT Head.
- Technical specifications will be provided by the ICT Department according to the user needs.
- In acquisition of ICT resources the ICT Department shall be involved in the procurement process that includes evaluation, inspection and acceptance.
- The ICT Department shall ensure all ICT resources are installed, configured, tested and Commissioned as per the requirements.
- ICT and SCMD shall ensure that all ICT equipment procured by or granted to the NLC shall be identified as belonging to the Commission, tagged or engraved for identification purposes before distribution.
- At distribution, all details shall be captured into an ICT asset inventory.
- The ICT Department shall use best practice and global standards and guidelines to develop technical specifications.

# CHAPTER 3: ICT SECURITY

## 3.1 Physical security policy

### 3.1.1 Purpose

To prevent unauthorized access or damage to hardware, software and information. This encompasses misuse, malicious or accidental damage, vandalism, intrusion, theft, undesired access and sabotage as well as natural disasters such as fire, water or earthquakes. This policy will ensure confidentiality, integrity and availability of data in case of unforeseen harmful events.

### 3.1.2 Scope

This policy shall apply to staff and third parties on protection and accessibility of physical ICT resources.

### 3.1.3 Policy

- The NLC shall provide access control and surveillance for the ICT key installations such as Data Center, active devices, cabinets and fiber channels.
- Data Centers shall be restricted areas, away from normal operations and only accessible to authorized personnel.
- Access control systems shall incorporate the use of biometrics for authentication.

### 3.1.4 Guidelines

### 3.1.5 Access to Computer Lab

- Only authorized staff shall work full time in computer lab.
- Other staff, vendors and maintenance personnel shall be provided with limited access on a need-to-enter basis.
- All visitors to the computer lab shall be escorted by an authorized staff and shall accompany the visitor until they depart.
- Computer lab must be locked when staff are not present, and the equipment shall be switched off at end-of-day or when not in use for extended periods.

### 3.1.6 Access to Data Centers

- Physical access to the Data Center areas must be controlled. Unauthorized persons shall not access the Data Centers
- Doors to Data Centers must be kept locked at all times and posted with “Restricted Area-Authorized Staff Only” signs. Only authorized staff shall be assigned keys to these areas. Other staff shall be provided limited access on a need-to-enter basis.

- All visiting delegations shall have prior appointments and must be accompanied by an authorized officer within these restricted areas.
- All entries and exits must be logged in a register which is always maintained at the entry of the Data Center.
- Contractors/suppliers must be accompanied by authorized officers and must enter their details in the entry/exit register.

#### 3.1.7 Theft Prevention of Equipment

- All theft or attempted vandalism must be reported to the administration by the affected party for investigation and further necessary action.
- After delivery of ICT equipment by vendors and prior to installation, arrangements should be made to house them in a secure and locked room.
- All equipment should be marked with identification denoting that it is the Commission's equipment.
- An inventory of ICT equipment shall be maintained by the ICT Department for ease of identification and location.
- No ICT equipment shall leave the Data Center and Computer lab without authorization by ICT Head.

### 3.2 Logical security policy

#### 3.2.1 Purpose

To enforce data integrity, confidentiality and availability.

#### 3.2.2 Scope

The policy applies to all users and data that belongs to the Commission.

#### 3.2.3 Policy

- All data is in the custody and under the stewardship of the Directorate/ Department originating them,
- The NLC shall provide access control mechanisms to protect access to systems, data and information,

#### 3.2.4 Guidelines

- Authorized access to data shall be through user accounts and password created by the systems administrator. Any access on need basis shall be through a written authority from the ICT Head.

- The NLC shall only allow access to data and information to Government agencies/users on request and limited for their use. The requesting person/agency/department must obtain authorization from the CEO/ Secretary.
- There shall be defined access levels, responsibilities, user rights, roles and privileges for all access to data.
- The access rights and levels shall be assigned by the systems administrator in liaison with Section and Department Heads and they shall be by segregation of duties.
- Access to systems shall be by use of passwords and biometrics where applicable.
- The security measures shall be strictly observed by ICT and all staff to protect critical, personal or sensitive data files from accidental or intentional disclosure to unauthorized users.
- All the users shall respect the privacy of other users' software and data.
- The NLC shall ensure that all external firms/agencies working on ICT systems or equipment that hold sensitive data, or with whom data is shared shall be required to sign non-disclosure agreements.
- The system administrator shall ensure that all users are joined in a domain environment for centralized management and administration

## 3.3 Password policy

### 3.3.1 Purpose

To protect and control access by users to ICT resources, systems and to establish a standard for creation and management of passwords and user accounts.

### 3.3.2 Scope

This policy applies to all users and systems at the Commission.

### 3.3.3 Policy

- All ICT resources shall be protected by use of passwords, access levels and segregation of duties.
- There shall be defined access levels, responsibilities, user rights, roles and privileges for all access to data.

### 3.3.4 Guidelines

- Access to systems and data must be protected by passwords. Only authorized persons will be given user accounts and passwords for access. This access is restricted to the user requirements appropriate to his or her job duties.
- The ICT Head shall be responsible for the administration of access controls to the NLC ICT systems and resources and shall process additions, deletions and changes upon receipt of a request from the user's supervisor.
- The ICT Head shall maintain a list of administrative access codes and passwords and keep this list in a secure area.
- Access to accounts and passwords shall be protected by each user of systems and shall not be written down.
- Users will be required to use passwords that comply to the following guidelines:
    - Passwords to accounts accessing or holding critical data shall be changed regularly and set to expire every thirty (30) days.
    - Passwords to accounts accessing or holding critical data shall not be reused in every twelve (12) months.
    - Users shall not disclose passwords to others. Password shall be changed if the user suspects that it is known to others or discovers a security breach.
    - All passwords must be strong, that is, incorporate capital letters, special characters and digits and be at least six (6) in total.
    - Passwords should not be simple and should not contain general information of the user such as anniversary dates or names of close family members or birthdates.
    - The system shall automatically log off a user after three (3) unsuccessful login attempts.

      **NB:** System administrators shall ensure strict compliance to these requirements.
- All users shall be responsible for all transactions made with their user ID and password.
- Automatic Log Offs - Systems should automatically log out and terminate idle sessions after three (3) minutes.

- Screen Locks – Users shall password-protect their screensavers so that in case they have to leave their desk/office unattended for a short period of time, the screen will automatically be locked until a password is entered.
- The ICT Head shall be notified by respective Directorate/ Departmental Heads when a user is transferred/dismissed/retires/resigns/on leave so that their user access can be revoked.
- Users shall not disclose passwords to third parties and the passwords must be changed immediately if it is suspected that they may have become known to others.

## 3.4 Antivirus policy

### 3.4.1 Purpose

To protect the Commission's ICT resources from attacks by malicious software such as computer viruses, worms, Trojan horses, spyware, root kits, botnet etc.

It is important to know that computer viruses are much easier to prevent than to cure and defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

### 3.4.2 Scope

This policy applies to all ICT resources and staff of the Commission.

### 3.4.3 Policy

- The NLC shall apply a dual anti-virus policy such that where there is connectivity, the NLC will install a corporate antivirus and areas where there is no connectivity, single user antivirus shall be installed.

### 3.4.4 Guidelines

The following guidelines are to assist in the prevention of virus attacks:

- The ICT Department shall:
  - Install and maintain appropriate licensed antivirus software on all computers.
  - Ensure regular updates and upgrades of the antivirus.
  - Respond to all virus attacks, eliminate any virus detected and document each incident and inform the users of infected computers of the action taken immediately.

- Update regularly antivirus software on standalone devices.
- Ensure that antivirus is enabled at all times.

➢ All staff shall:

- Not introduce a computer virus into computers whether knowingly or unknowingly.
- Not load removable storage of unknown origin into Commission computers.
- Scan removable media for viruses before being read.
- Immediately shut down the workstation and inform the ICT Department if they suspect that their workstation has been infected by a virus.
- Neither open nor forward attachments to an email from an unknown, suspicious or untrustworthy source. These attachments must be deleted immediately, and deleted again by emptying the recycle bin.
- Not download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless absolutely necessary.
- Regularly update the antivirus software.

## 3.5 BACKUP POLICY

### 3.5.1 Purpose

To establish the rules for the backup and storage of electronic information at the Commission. This policy is designed to protect data against loss and recover it in the event of an equipment failure, intentional destruction of data, or disaster.

### 3.5.2 Scope

This policy applies to all ICT resources and staff of the commission and to all core business data and systems, staff of the Commission, and external service providers who may be responsible for the installation, support and security of data and information.

### 3.5.3 Policy

All Commissions' systems data shall be backed up and securely stored on site, Data Recovery Site and off site.

### 3.5.4 Guidelines

- The ICT head shall ensure that backup and recovery procedures for each system are documented and periodically reviewed.
- Secure backups shall be taken on external media and may incorporate data encryption.
- Backups shall be stored on site and off site securely.
- Backups shall be protected using secure fireproof safe cabinets.
- Physical access controls shall be implemented at offsite backup storage and these locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest sensitivity level of information stored.
- A process must be implemented to verify the success of the backups
- Backups must be periodically tested to ensure that they are recoverable.
- Authorized staff access lists to offsite backup storage must be reviewed annually or when an authorized individual leaves the NLC or Department.
- Procedures between the NLC and the offsite backup storage administration must be reviewed annually.
- Backup tapes/storage must have the following minimum identification criteria by either labels and/or a bar-coding system:
  - System name
  - Creation date
  - Sensitivity classification
  - Retention regulations
  - Contact information
- System codes, configurations data, installations kits shall be part of data to be backed up and stored both onsite and offsite.
- All ICT systems delivered to the NLC shall have backup components.
- The System Administrator shall be responsible for:
  - performing and verifying backups for core systems,
  - checking that they have been successfully completed,
  - recording the information on the backup register,
  - ensuring that the backups are stored securely,
  - ensuring that the backup media are properly labeled and rotated,

- advising the SCMD Department on requirements for backup media.

## 3.6 INCIDENT REPORTING POLICY

### 3.6.1 Purpose

To ensure that incidents that may harm ICT resources are reported to relevant authorities.

### 3.6.2 Policy

All ICT related incidents shall be reported to the assigned duty officers/Supervisor/ Department/Directorate Heads or other officer as shall be advised by the Commission.

### 3.6.3 Guidelines

All security violations related to ICT shall be reported as:-

- Incidents of theft, attempted theft and malicious physical damage shall be reported to the Head of the directorate affected, administration and ICT Head.
- Incidents of data security breaches shall be reported to the ICT Head who shall in turn report to the Departmental Head for appropriate action.

# CHAPTER 4: ENVIRONMENT

## 4.1 Environmental control policy (Data center)

### 4.1.1 Purpose

To ensure that employees and systems are secured from environmental exposure due to natural occurring events and to control the environment in which the systems are implemented.

### 4.1.2 Scope

Applies to all the staff in the NLC and third parties.

### 4.1.3 Policy

The NLC shall endeavor to put safety measures at all levels and all times.

### 4.1.4 Guidelines

- **Hand-held** fire extinguishers shall be placed in strategic positions in the Data Centers. They shall be tagged for inspection and inspected annually.
- **Smoke Detectors** shall be placed above and below the ceiling tiles throughout the facility and below the raised Data Centers. They shall produce an audible alarm when activated.
- **Fire suppressors** shall be installed that removes oxygen from the air, thus starving the fire. The system should not damage the equipment.
- **Regular inspection by the contractors or suppliers** shall ensure that all fire detection systems comply with building codes. The relevant department shall inspect the system and facilities annually.
- **Fireproof walls, floors and ceiling** surrounding the Data Centers shall contain or block fire from spreading. The surrounding walls shall have at least a two-hour fire resistance rating.
- **Emergency power – off switch** to computers and peripherals shall be shut off in case of an emergency evacuation.
- **Data Centers** should have raised floor, floor tiles and not carpeted to minimize dust.

## 4.2 Health and safety policy

### 4.2.1 Purpose

To ensure that staff using NLC ICT resources are doing so in a healthy manner and in a safe environment.

### 4.2.2 Scope

This policy applies to all staff using the NLC ICT resources.

### 4.2.3 Policy

The NLC shall:

- Provide a healthy and safe environment for staff using ICT resources.
- Ensure that there is a system in place for regular health and safety checks (that will include visual checks of plugs, leads and other electrical equipment).
- Ensure that the laid down guidelines on health and safety are adhered to.

### 4.2.4 Guidelines

#### *Comfort*

- The NLC shall provide the recommended working tools for computer use.
- Users should be comfortably positioned, with ease of access to equipment. While sitting, users must be able to adjust their position in relation to the equipment as appropriate.
- Users should change posture frequently and take frequent ten minute breaks away from the computer to stretch their limbs and rest their eyes.

#### *Desks and workstations*

There should be enough space around a workstation for paper, books and other working tools. Desk design should take care of cable management. Gangways and emergency exits must be kept clear.

#### *Sitting*

When using ICT equipment, users need to sit at the recommended height (with the eye level at the top of the screen).

#### *Monitors*

Monitors should tilt and swivel to suit the requirements of individual users. The top of the screen should be roughly at eye level. Screens should be positioned to reduce

reflection and glare from lights and windows and should be adjustable for brightness and contrast as the lighting changes throughout the day. Clean screens give better visibility

and reduce glare. Screen distortion may occur if speakers are placed too close to the monitor, so it is advisable to position them about 30cm away.

### *Keyboards*

Users should have the option of using the keyboard flat or tilted. It is important for users to develop a good keyboard technique; Do not bend hands up at the wrist when typing, keep a soft touch on the keys and do not over-stretch your fingers. Straining may cause Repetitive Strain Injury (RSI - upper limb disorders including pains in the neck, arms, elbows, wrists, hands and fingers), a painful condition which has the potential to cause irreversible problems.

### *Screen projectors*

When using a data projector, make sure that equipment is supervised at all times during the projector's operation. One should never stare directly into the beam of the projector. When entering the beam, one should not look towards the audience for more than a few seconds. Careful consideration must be given to factors such as positioning and if possible, keep one's back to the beam at all times.

### *CD ROMs and DVDs*

Defective CD-ROMs or DVDs used in high-speed drives can shatter and allow pieces of disk to escape from the drive. To check that disks are in perfect condition, hold them up to the light and examine them for cracks, scratches or defects near the inner rim.

### *Noise*

Almost all ICT equipment emits background noise if the power is switched on, even when an item is not in use, and many software packages feature sound as part of their operation. The use of headphones may help to reduce distractions and aid concentration. Earphones should only be for personal use (for hygiene reasons).

### *Heat and Light*

The ideal temperature of an ICT suite is between 18 and 24 degrees Celsius, with humidity between 40 per cent and 60 per cent. Almost all ICT equipment gives off heat,

which can build up during the day and become quite oppressive for users, as well as detrimental to the equipment. Rooms must be well ventilated by using air conditioning if available, opening doors and windows and turning down the heat.

*Personal Safety*

- Users should be cautious when using specialized equipment such as shredders, Printers scanners, and photocopiers since fast-moving parts can trap clothing, jewelry and hair and may cause harm to them.

*Electrical Safety*

All electrical equipment should be maintained regularly. Technical repairs should be left to the experts. The location of electrical equipment depends on the length of cables and the availability of sockets. It is essential that the location of the equipment does not increase the risk of danger to equipment or users. Particular issues to be aware of are as follows:-

- Exposed power cables should be covered and secured,
- Frayed extension cables or damaged plugs should be replaced
- Circuits should not be overloaded, particularly when using extension cables, as power surging could occur if too many computers are connected to a circuit.
- Avoid coiled cables, as the heat generated within them could be sufficient to start a fire.
- Be aware of accidental damage, in particular any cuts to power cable insulation, and also damage from dust, spilt liquid.
- Ensure that the correct fuse rating is fitted.

*Mobile Equipment*

- The risk of lifting heavy or bulky equipment must be assessed and trolleys should be used where appropriate. It is advisable to push a trolley rather than pull it. When using mobile equipment such as projectors, they must be anchored firmly when in use.

*Hazardous substances*

- Risk assessment is necessary when using toners, printing ink and cleaning materials. Fluids used for cleaning and in some reprographic processes are flammable. They should not be used in confined spaces and adequate ventilation should be maintained.

# CHAPTER 5 HARDWARE, SOFTWARE AND CONSUMMABLES

## 5.1 Hardware policy

### 5.1.1 Purpose

To protect and maintain ICT hardware in the Commission so as to derive maximum value for the intended use and enhance efficiency and effectiveness in employees job performance.

### 5.1.2 Scope

The policy shall apply to all hardware in the Commission. The hardware includes: Personal Computers, Printers, Laptops, Servers, Scanners, Projectors, photocopiers, UPS', network switches, Digital Cameras among others.

### 5.1.3 Policy

- The ICT Department shall facilitate the acquisition, installation, configuration, testing, training and maintenance of equipment in the Commission.
- The use of foreign equipment in the NLC networks without the consent of the ICT Department is strictly prohibited.

### 5.1.4 Guidelines

- All procurement, inspections, evaluations, acceptance and distribution shall be undertaken in liaison with ICT for authorization, documentation and inventory management.
- All procured items shall come with warranties and user manual.
- The ICT Department shall maintain a list of standard hardware configuration for computers that are supported by the Unit subject to change as technology advances.
- Installation, configuration and training on procured equipment shall be done by the supplier, consultant or contractor in liaison with the ICT Department.
- The ICT Department shall manage all administrator accounts in computers and laptops while members of staff shall operate from user accounts.5.2 Software and licensing policy

### 5.2.1 Purpose

To ensure that software used in the NLC is in compliance with applicable licenses, notices, contracts and agreements to safe-guard NLC against any legal implications, benefit from support provided by the licenses.

### 5.2.2 Scope

This policy applies to all software developed or acquired for the purposes of NLC business functions. These include: operating systems, application software, database software, customized /off the Shelf software, computer drivers, Antivirus, and source code.

### 5.2.3 Policy

- All ICT equipment acquired and used in the NLC shall run on genuine and licensed software.
- All software acquired for or developed on behalf of the NLC shall be the property of the Commission.
- All software licenses shall be managed centrally by the ICT Department through Active Directory Environment.
- Source code for all application software developed for the NLC shall be the property of the Commission.

### 5.2.4 Guidelines

- Users shall request for software through the ICT head.
- ICT head shall maintain records of software licenses owned by the Commission
- ICT Department shall periodically scan computers to verify that only authorized software is installed
- All software is strictly controlled by the ICT Department in accordance with the provisions of the software licenses.
- NLC staff shall be individually responsible for reading, understanding and following applicable licenses, notices, contracts and agreements for software usage on Commission computers. The staff shall not:
    a) Install software without authority by the ICT Head
    b) Copy software unless authorized by the ICT Head.
    c) Download software unless authorized by the ICT Head.

### *Acquisition*

- Acquisition of software shall be co-coordinated with the ICT Department to ensure that it conforms to corporate standards.
- All software acquired shall have accompanying licenses and user manuals.
- Inspection, evaluation, acceptance, installation, configuration and Commissioning shall be done in liaison with ICT Department.

*Release of Software*

- Software shall not be loaned, traded, sold, given away, or otherwise divulged. Copies of Commission or leased software and data can only be released from ICT Department for non-Commission use with the written approval of the CEO/ Secretary.
- Any upgrading and updating of software will be done by the ICT Department.

*Custody of the software*

- ICT Department shall have custody of all software in the Commission.
- ICT Department shall facilitate training on the acquired software where necessary.
- The NLC staff shall not borrow or lend any software without the consent of Head ICT.
- All software developed in house by the NLC staff shall become the property of the Commission. However, there shall be due recognition of innovativeness.

*Licenses*

- The NLC shall comply with all laws regarding intellectual property. This applies to all Software licensed or developed in the Commission.
- The NLC may negotiate for corporate licenses where necessary.
- All purchased/customized software must be accompanied by the required licenses as per specifications.
- All registered licenses shall bear the name of the Commission.
- All purchased/customized software shall be delivered with documentation.
- All software revision shall be accompanied by documentation.

*Source Code*

It shall be the obligation of the contractor to provide the source code in an escrow account and ensure that updates are provided to the NLC when changes are made on the systems.

*Renewal of support licenses*

The ICT Department shall negotiate for the renewals of licenses on behalf of the NLC in liaison with the SCMD.

## 5.3 Intellectual property rights

### 5.3.1 Purpose

To protect the possibility of inadvertent infringement of the Intellectual Property Rights of software developed in-house or by third parties using or implementing any NLC customized specifications.

### 5.3.2 Scope

All system developers, staff from within or without the NLC and all third parties contracted to develop software and systems for the Commission.

### 5.3.3 Policy

- All systems and software developed for NLC use shall be copyrighted by the NLC on acceptance and handover of the system.
- Third party copyrighted software used by contractors engaged by the NLC as third party software shall retain copyright ownership of its original work, while at the same time granting the NLC a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Contractor's copyrights in its project delivery to reproduce, distribute, publish, display, perform, and create derivative works of the project based on that original work for the purpose of developing software or systems under the Commission 's copyright.
- Users accessing web based applications using the internet are not permitted to use false information or copy, transfer, rename, add or delete programs belonging to others unless given express permission to do so by the owner.
- Users shall observe copyright or license agreements.

## 5.4 Warranty policy

### 5.4.1 Purpose

To ensure that the warranty given to the NLC by contractors and suppliers stating that a product is reliable and free from defects is kept, and that the contractor/supplier will, without charge, repair or replace defective parts within a given time limit and under conditions agreed upon.

### 5.4.2 Scope

This policy shall cover all ICT resources acquired by the Commission.

### 5.4.3 Policy

- All ICT resources acquired by the NLC shall come with a written warranty.
- The NLC shall undertake to ensure warranties are honored.

### 5.4.4 Guidelines

- During preparation of ICT equipment specifications, warranty requirement shall be clearly defined.
- During delivery and inspection of ICT equipment, ICT Department shall ensure that warranty is provided for as per the specifications.

#### *ICT equipment*

- ICT equipment shall come with a warranty from the contractor who is an authorized dealer.
- The contractor/supplier shall support the ICT equipment within the warranty period.

#### *Software*

All software acquired for the NLC must come with the warranty for a specified period.

#### *Network infrastructure*

- All networking equipment must come with a warranty from the contractor who is an authorized dealer as per the specified period by the manufacturer.
- Contractors for network equipment shall be authorized dealers for active devices and shall have a manufacturer's authorization.
- The ICT Department shall verify the part numbers of active devices with the manufacturer where applicable.

## 5.5 Maintenance policy

### 5.5.1 Purpose

To provide for systematic inspection, detection and correction of evolving failures either before they occur or before they develop into major defects.

### 5.5.2 Scope

The policy shall cover all ICT equipment and accessories.

### 5.5.3 Policy

- The NLC shall ensure that preventive, corrective and adaptive maintenance plan is undertaken.
- The NLC shall ensure that the maintenance contracts and preventive plans are reviewed periodically to ensure that they meet the required standards.
- External service providers shall sign a non-disclosure agreement with the NLC when carrying out maintenance and repair services.

### 5.5.4 Guidelines

- Break down and/or malfunction of the ICT equipment shall be reported to the ICT Department
- Maintenance of ICT equipment will be coordinated by the ICT Department. Where the maintenance is to be performed by an external entity, the ICT Department shall advice accordingly.
- The ICT Department shall maintain documentation on maintenance operations for the Commission.
- ICT Head in liaison with SCMD shall prepare an ICT equipment maintenance contract and specification of the ICT equipment.
- ICT, SCMD and legal directorate shall maintain documentation and contracts on all ICT equipment maintenance undertaken by the Commission.
- Inventory of the machines which are out of warranty shall be maintained
- Preventive maintenance shall be done on all ICT equipment at least twice a year.
- ICT shall confirm acceptance and test for ICT equipment maintenance by preparing a report duly signed as stipulated in the contract.
- Maintenance of the network infrastructure shall be done at least twice per year for the active devices by an authorized manufacturer/dealer.
- Software contracts shall have a component of maintenance for a specified period of time.

## 5.6 Service level agreements (SLA) policy

### 5.6.1 Purpose

To ensure provision, performance and availability of ICT services and systems at all times. The Service Level Agreement (SLA) will be contracts between service provider(s) and the

Commission. The SLAs shall specify in measurable terms, the availability, timeliness and performance criteria that the contractor is intended to meet while delivering service and sets out the remedial action and penalties in case of violation.

### 5.6.2 Scope

The SLAs shall cover network infrastructure, customized systems, internet services, and all other ICT equipment.

### 5.6.3 Policy

- SLAs shall be prepared, discussed and negotiated by the NLC with the contractor.
- The Legal Officers from the NLC shall ensure that SLA contract documents meet the required contractual standards before signing.
- SLAs shall be reviewed annually.

## 5.7 Disposal policy

### 5.7.1 Purpose

To provide guidelines for the disposal of ICT hardware and software, and to provide data security and confidentiality during the process.

### 5.7.2 Scope

This policy covers ICT hardware and software that are owned or operated by the Commission.

### 5.7.3 Policy

- All ICT equipment that cannot be reused or serviced shall be forwarded to the ICT Department for assessment before forwarding for disposal.
- All disposed ICT equipment must be recorded and the asset inventory updated accordingly.

### 5.7.4 Guidelines

- All ICT devices shall only be disposed of after making sure that all the data or information is backed up and permanently erased.
- All ICT storage media shall be disposed of by demagnetizing and or physically destroying them.
- All ICT equipment to be disposed of must be certified by ICT Department that they are obsolete.

- Disposal of ICT equipment shall be undertaken by the Supplies Chain Management Department according to the Procurement and Disposal Act.
- ICT equipment have a lifespan after which a process for its disposal shall be put in place by ICT and SCMD.

# CHAPTER 6 ICT NETWORKS

## 6.1 Network infrastructure policy

### 6.1.1 Purpose

To centrally and strategically coordinate network infrastructure planning and implementation.

### 6.1.2 Scope

The policy covers all network infrastructures such as Local Area Networks, Wide Area Networks and Wireless Networks; active devices such as firewalls, switches, routers, DTUs; cabling, bandwidth, internet, access points, bridges and controllers.

### 6.1.3 Policy

- Network infrastructure shall be centrally planned, managed and maintained by the ICT Department.
- All network infrastructures shall incorporate security such as firewalls, VLANs, NAT, encryptions, VPNs, intrusion detection systems, Network Management System.
- Core systems data being transmitted over shared/public networks shall be encrypted.

### 6.1.4 Guidelines

- All requests from user Directorates/Departments for networks such as LAN, WAN and wireless connectivity shall be made to the ICT Head for assessment and technical specifications.
- The ICT Department shall conduct a feasibility study before technical specifications are developed.
- All default passwords for active devices must be changed, documented and kept in safe custody by ICT Head.
- The ICT Department shall ensure that network security is implemented in networks during data transmission.
- The ICT Department shall protect the networks and systems for which they are responsible and monitor performance.
- The ICT Department shall ensure that tests are carried out and review the results of automated network-based vulnerability, compromise assessment and guideline compliance scans of the systems and devices on NLC networks.

- The ICT Department and assigned security specialists shall constantly monitor network activity as necessary for detection of unauthorized activity and security against threats, intrusion attempts, and compromised equipment among others.
- ICT Department shall maintain network infrastructure designs, architectures, configurations and documentations.

## 6.1 Websites

### 6.1.1 Purpose

To ensure that the Commission's Information is provided online to the public.

### 6.1.2 Scope

This policy shall cover the websites developed and maintained by the Commission.

### 6.1.3 Policy

- It shall be the responsibility of the Office of the Public Communication of the NLC to update the website.
- The Head of ICT shall coordinate the development, upgrading and maintenance of the website and ensure that it is available for access.

### 6.1.4 Guidelines

- The ICT Head shall provide guidelines on the location to host the Commission's website.
- Content to be uploaded into the website shall be submitted to the Office of the Public Communication by the respective Directorates/ Departments as and when available.

## 6.3 INTERNET AND EMAIL POLICY.

### 6.3.1 Purpose

To provide secure access to internet and email services in the Commission for effective and secure communication.

### 6.3.2 Scope

This policy applies to all NLC staff and third parties who use internet and email services of the Commission.

### 6.3.3 Policy

*Internet*

- The ICT Department shall ensure that internet services are available to all members of staff
- The NLC shall put in place mechanisms to restrict access to unauthorized sites.
- Public internet access shall not be enabled on machines providing core business applications.

*Email*

- The NLC shall provide electronic mail accounts to its staff for use to conduct official business.
- All official electronic communications shall be done through official e-mail facility.
- The ICT Department shall put measures in place to protect the e-mail facility against misuse by staff.
- The NLC will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill the Commission's obligations to third parties.
- The commission shall have a standard email disclaimer which users must not remove or change when sending email messages.

### 6.3.4 Guidelines

- Head of HR shall forward names of officers who have joined/left the NLC for the purpose of creating or deleting e-mail accounts.
- Email addresses shall have the format first.Lastname@DomainName.or.ke.
  Where two or more employees share the same first and last name, use the Last and the First name approach.
- The ICT Department shall be responsible for creating the user accounts/emails of all the NLC employees
- All NLC staff shall have access to internet services for transactions on official matters.
- The officers shall be required to use official email addresses for official communications.
- The NLC shall provide a redundant link to support the primary network.
- Internet connection request shall be made to the Head of ICT.

### 6.3.5 Acceptable Use

- Users who use the NLC internet services from an e-mail account shall:
  - Ensure that all communications are for official use and do not interfere with his/her productivity.
  - Ensure that Internet is used in an effective, ethical, and lawful manner
  - Not use the Internet for purposes that are illegal, unethical, harmful to Commission, or non-productive.
  - Be responsible for the content of all text, audio, or images they place or send over the Internet.
  - Not transmit copyrighted materials without permission from the copyright owner.
  - Know and abide by all applicable policies dealing with security and confidentiality of records.
  - Run a virus scan on any attachments received through the internet.

### 6.36 Downloads

Downloading files and/or programs from the internet causes a potential systems threat. The responsibility of downloaded files or programs lies with the user. In case of doubt, users should contact the ICT Department.

# CHAPTER 7 SERVICE MANAGEMENT

## 7.1 User support policy

### 7.1.1 Purpose

To ensure that all Commission staff is accorded the necessary ICT support while using ICT resources.

### 7.1.2 Scope

This applies to all Commission staff.

### 7.1.3 Policy

The ICT Department shall endeavor to provide quality support to all users as per the ICT Department user support procedures.

### 7.1.4 Guidelines

- Users shall immediately contact the ICT Department when they have ICT related issues

## 7.2 Shared services policy

### 7.2.1 Purpose

To facilitate the sharing of services for cost effectiveness and interoperability.

### 7.2.2 Scope

The policy will cover resources that can be shared such as network infrastructure, Printers, Photocopiers, system applications, database and software licensing for purposes of maximizing the use of ICT resources.

### 7.2.3 Policy

- The NLC shall endeavor to identify, facilitate and consolidate all services that can be shared.
- All users shall share physical infrastructure such as network infrastructure, Data Centers, printers, photocopiers and scanners.

## 7.3 INVENTORY MANAGEMENT POLICY

### 7.3.1 Purpose

Facilitate the management of ICT equipment for the purpose of tracking, distribution, and repossessing which will also facilitate maintenance, disposal, forward budgeting and planning.

### 7.3.2 Scope

This policy covers all software, computer and communication devices, storage devices, documentation, equipment and accessories acquired by the Commission.

### 7.3.3 Policy

- The NLC shall create and maintain an inventory of all ICT resources which shall be updated regularly to provide the current status.
- All users leaving the NLC on retirement, dismissal or transfer shall surrender all ICT resources issued to them.

### 7.3.4 Guidelines

- All equipment and software purchased by the NLC shall remain the property of the Commission and shall be tagged appropriately.
- The ICT Department and SCMD shall maintain, manage and have custody of the inventory of all ICT equipment for the Commission.
- On delivery and acceptance of ICT resources, their details shall be entered into the inventory. Details which include: item, description, model, serial number, destination office and responsible staff.
- At distribution, details of the location, user, and the Directorate/Department shall be captured into the inventory.
- There shall be an ICT Equipment register to log movement of equipment to and from the Department.

## 7.4 DOCUMENTATION POLICY

### 7.4.1 Purpose

To ensure that all documentation for ICT resources is well-kept for referencing and continuity purposes.

### 7.4.2 Scope

The policy shall cover all documentation in the NLC that pertains to ICT systems and resources. The documentation includes among others:

1) Service Level Agreement
2) Contracts
3) Technical specifications document

4) Networks designs, architecture and configurations
5) Hardware and software documentation
6) Systems passwords and documentation
7) Project documentation
8) Test plans and Acceptance reports
9) System audit reports
10) Quality assurance reports
11) User requirements and systems Requirements
12) Source code
13) User manual
14) Installation and recoverable disks
15) Feasibility study report
16) report

### 7.4.3 Policy

- The NLC shall ensure ICT System/resources are documented.
- ICT Department shall keep such documents and make them easily available.
- Vendors/Contractors shall deliver all ICT resources/systems with accompanying documentation.

### 7.4.4 Guidelines

- Regular checks shall be carried out to ensure compliance by Monitoring and Evaluation teams to be appointed by the CEO/ Secretary.
- It shall be the responsibility of the ICT Department and SCMD to have custody of the documents.
- It shall be the responsibility of all contractors where applicable to provide documentation as indicated in the scope:
- Documentation shall be stored both in hard and soft copy where applicable.

## 7.5 ICT AUDIT POLICY

### 7.5.1 Purpose

To provide for conformity and adherence to the set policies and standards on matters related to ICT resources.

### 7.5.2 Scope

This policy covers all ICT resources under the custody of the Commission.

### 7.5.3 Policy

The Head ICT shall undertake annual system audits to establish conformity and adherence of ICT resources.

### 7.5.4 Guidelines

- Auditors shall be granted access to ICT resources for the purpose of performing an audit when needed.
- Independent consultants shall be involved in undertaking security checks for the network and systems.

## 7.6 PROJECT MANAGEMENT

### 7.6.1 Purpose

To ensure that there is common and consistent application of formal project management methodology, principles and practice in the Commission.

### 7.6.2 Scope

This policy covers all ICT projects that shall be undertaken by the Commission.

### 7.6.3 Policy

- All ICT projects shall be implemented in line with the objectives of promoting E-Governance.
- The CEO/ Secretary shall constitute an implementation team to oversee each ICT project.
- Implementation of any ICT project shall be done by a project implementation committee headed by a Project Manager who shall report to the committee.
- The NLC shall engage Quality Assurance services to ensure quality of the project.
- All projects must adhere to a project management methodology that will be prescribed by the ICT Head in liaison with the user Directorate/Department.
- All international contracted firms for the projects shall have a qualified local company that will provide support services to the project according to Public Procurement and Disposal Act.
- After completion of each project, a formal post-project review shall be undertaken by the NLC and the contracted firm to assess:
  - Overall success,
  - scope management,
  - quality of deliverables,

- key accomplishments,
- Problem areas and business process best practice established for continuous improvement.

# CHAPTER 8 CAPACITY BUILDING

## 8.1 ICT TRAINING POLICY

### 8.1.1 Purpose

To build capacity for members of staff of the Commission on ICT skills and competencies so as to ensure updated technologies are implemented and systems security is achieved.

### 8.1.2 Scope

This policy shall apply to the staff in the Commission.

### 8.1.3 Policy

- The NLC shall train the ICT staff in professional and industry certification courses.
- The NLC shall ensure that all ICT projects, hardware and software acquired shall have necessary training components as follows:
  - Technical user training
  - Professional training (Certifications)
  - Management user training
  - Operational user training
  - Trainers of Trainers (TOT)
- Commission shall facilitate ICT officers to attend relevant seminars, workshops within and without the country to enhance their skills and gain exposure to new and emerging technologies.
- The NLC shall ensure that all Commission staff will undergo a basic training for ICT skills.
- The NLC shall provide comprehensive training relating to the acquisition and disposal of ICT resources.
- The NLC shall provide comprehensive training to ICT Staff relating to the maintenance of ICT resources.
- The ICT Department shall train members of staff on emerging ICT Technologies from time to time.

### 8.1.4 Guidelines

- The NLC shall facilitate training and at least one workshop annually for ICT officers to update them on emerging Technologies.
- ICT Department shall ensure user manuals are available for training and reference purposes.

- ICT Department shall facilitate training for new users on how to use ICT tools for operations.
- The ICT Head shall facilitate induction of the newly recruited ICT officers.
- The ICT Head shall facilitate professional training for ICT staff.

# CHAPTER 9: PROHIBITION, RESTRICTION AND PENALTIES

## 9.1. PROHIBITION AND RESTRICTIONS

It is important for users to be aware of applicable laws and regulations when accessing or using data or systems that are internal or external to the commission. Areas of consideration should include but not limited to copyright, trademarks, patent, privacy, wiretap confidentiality and communication laws and regulations. Use of computing resources to violate laws or regulations represents violation of this ICT Policy.

The following activities are generally prohibited or restricted. Certain individuals may be exempted from these rules in order to perform their required job responsibilities (e.g. System administrators and Network administrators are authorized to actively monitor network traffic and respond in a disruptive manner to mitigate a detected threat). Employees are not authorized, under any circumstances, to actively engage in activities deemed illegal under applicable jurisdictions.

The list provided below is not comprehensive, but should be used as a baseline for helping determine whether or not a proposed action is unacceptable. Omission of an action from this list does not imply that it is an acceptable use. Any violations of these specific prohibitions and restrictions will be treated severely and may reasonably result in immediate termination of employment.

### 1. Illegal use

Computing resources must be used within the confines of the law. Any use of computing resources to infringe intellectual property protections, such as copyrights, trademarks, patents or trade secrets, is prohibited. Infringing acts may include, but are not limited to, unauthorized copying of copyrighted materials, use of a trademark without authorization or exporting software, technical information, encryption or technology in violation of export control laws. Any action, intentional or unintentional, that serves to copy or transmit protected materials without proper authorization is an unacceptable use.

### 2. Threats or harassment

Computing resources must not be used to threaten, harass or harm others. Unauthorized uses of this type may include, but are not limited to:

• Communication that is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, tortuous, or containing explicit or graphic

descriptions or accounts of sexual acts (including but not limited to sexual language of a violent or threatening nature directed at another individual or group of individuals);

• Communication that victimizes, harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, gender, sexual orientation, race, ethnicity, age, or disability;

• Any form of harassment via email, telephone, paging or instant messaging, whether through language, frequency, or size of messages;

### 3. Fraud, forgery or impersonation

Any use of computing resources to commit fraud, forgery or impersonation is strictly prohibited. All users must truthfully and accurately represent their identity at all times. Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers, including email header information, or other identifying information is prohibited.

Postings to public places intended to mask your employment status and employer, may be allowed.

### 4. SPAM / SPIM

Creation, sending and forwarding of unsolicited advertising, junk or bulk email ("SPAM") or instant messages ("SPIM") are strictly prohibited, unless explicitly authorized as part of your normal job duties. Undertaking any activities that serve to facilitate unsolicited commercial email or unsolicited bulk email, whether or not that email is commercial in nature, are prohibited. Use of instant messaging facilities to accomplish the same is also prohibited.

### 5. Unauthorized access or circumvention of access controls

Any access to systems or data that is not specifically authorized is prohibited. Any circumvention of access controls, whether for accessing systems with or without authorization, is also prohibited. Users may not circumvent authentication or security of any host, network or account.

## 6. Collection of confidential data

Use of computing resources to collect confidential data, such as about members, employees or intellectual property, is prohibited. Collection, or attempts to collect, personal information about third parties, without their knowledge or consent, is prohibited and may constitute a violation of Commission privacy policies and agreements. The Commission strictly limits its liability in cases where individuals act on their own accord and without proper authorization. Any attempts to harvest or collect confidential data without explicit and proper authorization is prohibited and will be subject to severe disciplinary actions, up to and including termination of employment.

## 7. Disrupting network services or access to data

Rendering systems, networks, applications or data inaccessible or unusable due to an unauthorized disruption or corruption, is prohibited. Such prohibited acts may include, but are not limited to, ping floods, packet spoofing, executing denial of service or distributed denial of service attacks, forging routing information, corrupting data upon which an application or system relies, or removing or disabling a service, such as a process or application, on a host or network. Port or security scanning without prior authorization by operations security is strictly prohibited. Using any automated tool, such as a program, script or command, to send any message with the intent to interfere with or disable terminal sessions is not acceptable.

## 8. Disclosure of protected information

Disclosing Commission confidential information is prohibited. Disclosures may include, but are not limited to, unique account names, account passwords or lists of employees, contractors, consultants, vendors or products. All information must be treated as confidential and protected unless labeled otherwise.
Certain information may be disclosed, including email address, assigned desk phone number, fax number, mailing address or title.

## 9. Monitoring or interception of network traffic

Monitoring or intercepting any form of network traffic or data not intended for your own host is prohibited, unless authorized as part of your normal job duties. Monitoring

or intercepting network traffic may violate the privacy or confidentiality of the data being transmitted.

## 10. Introduction of network services or routing configurations

The introduction of routing patterns or network services that are inconsistent with established patterns or services and/or that may disrupt or interfere with the intended patterns or services are expressly prohibited. Examples of unacceptable use include, but are not limited to, broadcasting routing information, providing Dynamic Host Control Protocol (DHCP) services in conflict with authorized services, or sending network messages designed to terminate network connections (such as TCP RST packets, or "sniping").

## 11. Release of information regarding security incidents

Authorization to release information regarding security incidents involving the Commission is restricted solely to management and its assigned agents (e.g. legal counsel or public relations agents). In the event of a security incident involving the Commission, individuals are not authorized to communicate news of such incidents to any outside party. It is solely the Commission's responsibility to appropriately notify public of security incidents in compliance with government regulations.

## 9.2 Penalties

By accepting employment with the Commission and using computing resources owned by the Commission, the user is accepting the terms of this ICT Policy and agreeing to abide by its provisions

Failure to observe policies and guidelines in this ICT policy may result in disciplinary action by the Commission and/or legal action.

Action will be taken in accordance with relevant Government Policies, Code of Regulations as appropriate, and the involvement of the Police and/or other law enforcement agencies.

Action may be taken against any officer who contravenes the requirements of this policy as per:

- The Code of Regulations ……
- Public Service Regulations Act ……
- Ethics and Anti-Corruption Act 2003….