REPUBLIC OF KENYA

NATIONAL EMPLOYMENT AUTHORITY

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

JUNE, 2023

I DOCUMENT FORMULATION AND REVISION HISTORY

Version	Date	Author(s)	Revision Notes
1.0	March 2020	ICT Department	Initial draft
1.1	June, 2020	ICT Department	Final Policy document
1.2	June, 2023	ICT Department	Final Policy document
1.3			
1.4			
1.5			
1.6			
1.7			

II. FOREWORD

The National Employment Authority has procured and implemented Information and Communication Technologies (ICTs) that are used to create, process, store, share and disseminate data and information. These are assets which represent a significant economic investment by the Authority. The data and information resources they create, store and disseminate are priceless and may be irreplaceable. Their continued availability in furtherance of the Authority's core business is of paramount importance, hence, there is a compelling need to secure and control access to them.

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

Confidentiality of information is demanded by the government regulations and conventions. Since the Authority operates as a government institution dealing in Management and Promotion of Employment services that entails handling stakeholder's data, misuse of the institution's ICT assets could degrade its goodwill and reputation.

The Authority 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 Authority 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.

The ICT policy is a positive by NEA in addressing the underlying Information Communication Technology challenges. The policy will guide the Authority in delivering on its mandate.

I wish to encourage the staff of NEA to utilize this policy ICT in order to improve access to information and make communication easier and more efficient.



EDITH OKOKI (MRS)

Ag. DIRECTOR GENERAL

TABLE OF CONTENTS

I DOCUMENT FORMULATION AND REVISION HISTORY i

II. FOREWORD ii

IV. ACRONYMS AND ABBREVIATIONS viii

V. INTRODUCTION ix

NATIONAL EMPLOYMENT AUTHORITY x

MANDATE OF THE AUTHORITY x

CORE FUNCTIONS x

VISION xi

MISSION xi

CORE VALUES xi

ICT DEPARTMENT xii

FUNCTIONS OF THE ICT DEPARTMENT xii

LEGAL AND REGULATORY FRAMEWORK xiii

VISION xiii

MISSION xiii

ROLES AND RESPONSIBILITIES xiii

CHAPTER 1: OVERVIEW 1

1.1. The Policy Overview 1

1.2. Policy document approval and distribution 1

1.3. Accessibility 1

1.4. Policy revision 1

1.5. Scope of policy 1

Policy Statement 2

Policy Guidelines 2

Enforcement 3

1.6. User ethics 3

1.7. Responsibilities 4

1.8. Accounting Officer 4

1.8.1. Directorate/ Departmental/ Section Heads 4

1.8.2. The ICT Head: 4

1.8.3. The staff 5

1.8.4. The Systems Administrators/ ICT Officers shall 5

CHAPTER 2: ICT USE 6

2.1. ICT resource use policy 6

2.1.1. Purpose 6

2.1.2. Scope 6

2.1.3. Policy 6

2.1.4. Guidelines 6

2.2. Acquisition of ICT resources policy 7
2.2.1 Purpose 7
2.2.2 Scope 7
2.2.3 Policy 8
2.2.4 Guidelines 8
CHAPTER 3: ICT SECURITY 9
3.1 Physical security policy 9
3.1.1. Purpose 9
3.1.2. Scope 9
3.1.3. Policy 9
3.2 Guidelines 9
3.2.1 Access to Computer Rooms 9
3.2.2 Access to Server Rooms 9
3.2.3 Theft Prevention of Equipment 10
3.3. Logical security policy 10
3.3.1. Purpose 10
3.3.2. Scope 10
3.3.3. Policy 10
3.3.4. Guidelines 11
3.4. Password policy 11
3.4.1. Purpose 11
3.4.2. Scope 11
3.4.3. Policy 11
3.4.4. Guidelines 12
3.5. Antivirus policy 13
3.5.1. Purpose 13
3.5.2. Scope 13
3.5.3. Policy 13
3.5.4. Guidelines 13
3.6. Backup policy 14
3.7. Incident reporting policy 15
3.7.1 Purpose 15
3.7.2 Policy 15
3.7.3 Guidelines 15
CHAPTER 4: ENVIRONMENT 16
4.1. Environmental control policy 16
4.2. Health and safety policy 16
4.2.1. Purpose 16
4.2.2. Scope 16
4.2.3. Policy 17

4.2.4. Guidelines 17
CHAPTER 5: HARDWARE SOFTWARE AND CONSUMMABLES, ... 21
5.1 Hardware policy 21
5.1.1 Purpose 21
5.1.2 Scope 21
5.1.3 Policy 21
5.1.4 Guidelines 21
5.2 Software and licensing policy 22
5.2.1 Purpose 22
5.2.2 Scope 22
5.2.3 Policy 22
5.2.4 Guidelines 22
5.3 Intellectual property rights 24
5.3.1 Purpose 24
5.3.2 Scope 24
5.3.3 Policy 24
5.4 Warranty policy 25
5.4.1 Purpose 25
5.4.2 Scope 25
5.4.3 Policy 25
5.4.4 Guidelines 25
5.5 Maintenance policy 26
5.5.1 Purpose 26
5.5.2 Scope 26
5.5.3 Policy 26
5.5.4 Guidelines 26
5.6 Service Level Agreements (SLA) policy 27
5.6.1 Purpose 27
5.6.2 Scope 27
5.6.3 Policy 27
5.7 Disposal policy 28
5.7.1 Purpose 28
5.7.2 Scope 28
5.7.3 Policy 28
5.7.4 Guidelines 28
CHAPTER 6 : NETWORKS 30
6.1. Network infrastructure policy 30
6.1.1. Purpose 30
6.1.2. Scope 30
6.1.3. Policy 30

6.1.4. Guidelines **30**
6.2. Websites 31
6.2.1. Purpose **31**
6.2.2. Scope **31**
6.2.3. Policy **31**
6.2.4. Guidelines **31**
6.3. Internet and email policy 32
CHAPTER 7: SERVICE MANAGEMENT **34**
7.1. User support policy **34**
7.1.1. Purpose **34**
7.1.2. Scope **34**
7.1.3. Policy **34**
7.1.4. Guidelines **34**
7.2. Shared services policy **34**
7.2.1. Purpose **34**
7.2.2. Scope **34**
7.2.3. Policy **35**
7.3. Inventory management policy **35**
7.3.1. Purpose **35**
7.3.2. Scope **35**
7.3.3. Policy **35**
7.3.4. Guidelines **35**
7.4. Documentation policy **36**
7.4.1. Purpose **36**
7.4.2. Scope **36**
7.4.3. Policy **37**
7.4.4. Guidelines **38**
7.5. ICT audit policy **38**
7.5.1. Purpose **38**
7.5.2. Scope **38**
7.5.3. Policy **38**
7.5.4. Guidelines **38**
7.6. Project management **38**
7.6.1. Purpose **38**
7.6.2. Scope **39**
7.6.3. Policy **39**
CHAPTER 8: CAPACITY BUILDING **40**
CHAPTER 9: PENALTIES **42**
9.1. Penalties 42
APPENDICES 43

APPENDIX I: ICT POLICY COMPLIANCE AGREEMENT..... 43
APPENDIX II:ICT EQUIPMENT MOVEMENT SAMPLE REGISTER 44

IV. ACRONYMS AND ABBREVIATIONS

CD-ROM	–	Compact Disc - Read only Memory
DEG	–	Authority of E-government
NEA	–	National Employment Authority
DTUs	–	Data Terminal Department
DVD	–	Digital Versatile Disc
GCCN	–	Government Common Core Network
GOK	–	Government of Kenya
HOD	–	Head of Department
HRM(S)	–	Human Resource Management Services
ICT	–	Information and communication Technology
ISO	–	International Standards Organization
LAN	–	Local Area Network
VLANs	–	Virtual Local Area Networks
VPNs	–	Virtual Private Networks
WAN	–	Wide Area Networks
MDAs	–	Ministries, Departments and Agencies
PDA	–	Personal Digital Assistant
SCMD	–	Supply Chain Management Department
SLA	–	Service Level Agreements
TOT	–	Training of trainers
UPS	–	Uninterruptible power supply

V. INTRODUCTION

Information and Communications Technology (ICT) is the use of computing and telecommunication technologies, systems and tools to facilitate the way information is created, collected, processed, transmitted and stored. It includes computing technologies like servers, laptop computers and software applications, as well as the wired and wireless communication technologies that support telephones, the Internet. The goal of embracing ICT is to improve access to information and make communication easier and more efficient.

The Automation of the National Employment Authority services is part of the wider Government program to computerize and bring services closer to the citizens. The Authority is deliberately undertaking service transformation through the use of ICT to effectively and efficiently serve its customers who mainly include employers, job seekers and Private Employment Agencies. In order to provide transparent, efficient and accountable systems, the Authority has invested heavily in providing tools required to perform these functions. This can only be achieved by providing the staff with access to electronic equipment and services such as computers, email, internet and business support systems. Further, the Authority is building capacity 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 Authority 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 policy document is set out to provide guidelines and procedures to the members of staff and third parties in the Authority on matters related to ICT use, and also to ensure compliance to the same.

NATIONAL EMPLOYMENT AUTHORITY

MANDATE OF THE AUTHORITY

The Mandate of the Authority is to:

a) Provide a framework and facilitation of employment of Kenyans in the private sector;

b) Provide a framework to facilitate increased employment of Kenyans in the national government, county governments, state organs, and national and county government entities;

c) Promote foreign employment to absorb excess labour force;

d) Provide for the maintenance of a database of all Kenyans seeking employment;

e) Facilitate and promote equity and diversity, and eliminate discrimination in employment of Kenyans;

f) Give effect to the constitutional values and principles in matters of employment;

g) Give effect to Articles 55(c) and 56(c) of the Constitution;

h) Facilitate and track employment creation; and

i) National employment policy management.

CORE FUNCTIONS

The functions of the Authority are provided under Section 8 of the National Employment Authority Act, 2016. In the section, the National Employment Authority's functions shall be to:

1. Advise on formulation of employment policies and strategies for national and county governments;
2. Advise both the national and county governments on any policy matter concerning employment;
3. Develop methodologies for employment measurement, management and promotion;
4. Conduct periodic surveys on labour market skills requirements and advice training institutions and job seekers appropriately to ensure that training and skills match the job market requirements;
5. Monitor implementation of employment policies and programmes;

6. Facilitate cooperation with national government, the private sector, the informal sector and foreign governments and institutions to promote and increase access to employment;
7. Facilitate continuous training and other activities of Kenyans to improve their chances of employment and work skills;
8. Register persons seeking employment;
9. Maintain an integrated and up-to-date database of all persons seeking employment;
10. Facilitate the employment and placement of jobseekers in formal and informal or any other form of employment, locally and internationally;
11. Circulate in a timely manner job vacancies advertized to job seekers throughout Kenya through appropriate means including use of social media, internet and published materials;
12. Provide counseling to the unemployed and undertake activities to promote employment;
13. Facilitate the implementation of national policies on employment;
14. Take necessary steps to encourage equal opportunity employment practices for the benefit of the unemployed;

VISION

"Employment opportunities for all"

MISSION

"To formulate and implement employment policies and programmes for creation of sustainable employment for all Kenyans."

CORE VALUES

The Authority is committed to upholding the following Core Values as the guiding principles for operations in the medium and long-terms:

1. **Equity and diversity in access to employment opportunities** – NEA will ensure equity and diversity in access to employment opportunities for all Kenyans
2. **Participation of stakeholders** – The Authority promotes commitment and participation by all stakeholders in development and implementation of employment programmes.

3. **Creativity and Innovativeness** – NEA will develop programmes that promote sustainable employment opportunities among the youth
4. Customer Focus – NEA is committed to uphold customer-driven and customer focused services that deliver results to all
5. Integrity, Transparency and Accountability – The Staff shall uphold the highest and ethical standards while ensuring openness and responsibility for results to its customers.

ICT DEPARTMENT

The ICT Department is responsible for all matters pertaining to ICT such as coordinating, supervising, quality control, training, user support, development and management of the Authority's website, automation of business processes, and provision of technical advice on ICT issues. 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 Authority 's network infrastructure.

For this to be achieved there is need to have an ICT policy in place. This policy aims at providing the framework for developing and maintaining an effective information communication technology environment.

FUNCTIONS OF THE ICT DEPARTMENT

The primary role of the Department is to provide ICT services to the Authority through the following functions and responsibilities among others;

- Coordinating development and implementation of the Authority's ICT policy and strategy;
- Formulation of ICT policy;
- Implementing e-Government initiatives;
- Maintaining ICT standards within the Authority;
- Application of ICT, systems analysis and design;
- Carrying out research & development on ICT standards, guidelines & approaches and coordinating their consistent and efficient application in the Authority;
- Developing and implementing computerized information systems;
- Formulating and developing the Authority's information infrastructure;
- Training on the use of computers, relevant software packages and developing customized applications;
- Coordinating and developing the Authority's website;

- Providing advisory services on all matters related to ICT;
- Providing hardware maintenance support services; and
- Liaising with hardware vendors for administration of guarantees and warranties.

LEGAL AND REGULATORY FRAMEWORK

This policy has taken into consideration the following existing legal and regulatory provisions among others: -

1. Data Protection Act 2019
2. National Employment Authority Act of 2016
3. Private Employment Agencies Regulations
4. Labour Institutions_Act,2007
5. Employment_Act_2007
6. Legal Notice 110 – Labour Institutions Act 2007
7. National ICT policy
8. ICT Masterplan

VISION

To be the lead provider of ICT Services in the public service.

MISSION

To leverage the use of information and communication technologies in assisting provision of strategic leadership and guidance to the Authority on employment services and provide an enabling environment for ICT to thrive.

ROLES AND RESPONSIBILITIES

a. Board of Directors

i. Approval of the ICT policy.

b. Accounting Officer

i. Provide resources to purchase and license the required hardware and software.
ii. Provide adequate staff to manage infrastructure.
iii. Enforcement of the ICT policy.

c. Head of ICT

i. Sensitize all NEA staff on the ICT Policy;

ii. Ensure coordination, implementation and compliance of the policy.

iii. Provide support and guidance to users in understanding their responsibilities with regard to the policy.

iv. Recommend /advise on the appropriate controls to be acquired.

d. Human Resources

i. Providing timely information regarding new employees and termination or variation of employment status to managers and system administrators.

ii. Enforce penalties on non-conformity in line with the NEA HR policy and procedures manual.

e. Heads of Departments

i. Ensure that all users under their supervision are aware of this policy.

ii. Notify the ICT Department whenever there is a breach of the policy in their functional areas.

f. User Responsibilities

i. Understand and adhere to the policy.

ii. Notify any breach of policy to the ICT Department.

CHAPTER 1: OVERVIEW

1.1. The Policy Overview

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

The specific objectives of this policy are to:

- Identify priority areas for ICT development.
- Provide guidelines on acquisition, use and disposal of ICT equipment.
- Establish standardized guidelines for the use of government's ICT resources at the Authority.
- Protect the Authority's ICT infrastructure, data and business processes.
- Promote use of ICT in service delivery
- 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 Authority.

1.2. Policy document approval and distribution

Upon approval of this document by the NEA Board, the policy will be disseminated to all Heads of Directorates, Departments and Sections. They shall in turn ensure that all users read and adhere to the policy. The document will be distributed both in soft and hard copies.

1.3. Accessibility

It is intended that this ICT Policy is accessible in its entirety at Departmental and Section Heads' Offices, Authority's intranets, ICT Department and the library.

1.4. Policy revision

The document will be reviewed 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. Scope of policy

The scope of this policy focuses on staff and ICT resources including hardware, software, licensing, maintenance, warranty, intellectual property rights, training, standardization and acquisition.

This policy therefore is established in order to:

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

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

Policy Statement

This policy shall be in accordance with the Government of Kenya ICT Governance Standard and other industry best practices. It aims at providing strategic alignment of ICT services to the business objectives of the Authority.

Policy Guidelines

a) The Accounting Officer shall setup an ICT steering committee at the management level in line with ICT governance standards to provide an oversight on issues related to ICT.
b) The Head of ICT shall prepare and maintain an ICT strategic plan to improve services to internal and external clients.
c) The Head of ICT shall ensure that ICT projects are conducted as per the ICT Masterplan
d) The Head of ICT shall develop and properly disseminate an ICT service charter for all ICT enabled services.
e) The directorate of strategy and quality management in conjunction with Head of ICT shall conduct and document customer satisfaction surveys on ICT enabled services for internal and external clients.
f) The Head of procurement in liaison with Head of ICT shall develop and sign service level agreements (SLAs) with all ICT service providers to ensure reliability and availability of outsourced ICT services.
g) The Head of ICT shall establish an ICT service desk management system to handle all support requests from end users.
h) Head of ICT shall develop and implement quarterly preventive maintenance plans for ICT equipment.

i) The Head of ICT shall develop and maintain manuals on how to operate and maintain systems and equipment.

j) The Head of ICT shall establish an information security management framework as guided by the Information Security Management System (ISMS)

k) The Head of ICT shall implement an ICT knowledge base which shall contain a database of common ICT service problems and their resolutions.

l) The Audit Department shall conduct regular system audits for all systems to ensure compliance and conformity to the ICT standards. Where necessary the Authority shall engage ICT Authority for the audits.

m) The legal department shall advice whenever engaging in challenging, risky and complex contracts for ICT service provision.

n) The Head of ICT shall undertake ICT risk management as guided by the ICT governance standard.

o) The Accounting Officer shall ensure that there are enough resources to manage ICT services and projects.

p) The management shall document the decision to acquire external support as well as develop a framework for the accounting of the consultancy, contracting and external service providers.

Enforcement

NEA shall ensure compliance to this policy but the overall Authority rest with the Board of Directors

1.6. User ethics

- 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.
- The ICT resources provided to staff for the purpose of conducting Authority's core business must be used responsibly. Misuse of these resources will lead to disciplinary action.
- Any action that may lead to exposure of NEA data, unauthorized access to data, and 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 shall refrain from engaging in any activity that would subject the NEA to any liability. The Authority 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 NEA ICT assets and its users against unauthorized or improper use and to investigate possible violation of NEA rules and policies, measures shall be put in place.
- The Authority 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 Authority's rules or policies.
- The Authority 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.

All users are expected to read and sign the ICT Security Compliance Agreement (***Appendix 1***).

1.7. Responsibilities

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

1.8. Accounting Officer

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

1.8.1. Directorate/ Departmental/ Section Heads

Shall facilitate the implementation of the policy within their departments.

1.8.2. The ICT Head:

1) In liaison with Heads of Departments and Sections, the ICT Department shall ensure that all users are aware of and comply with the policy.
2) Shall create appropriate 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.

1.8.3. The staff

1) Shall safeguard the ICT equipment in their custody.
2) Shall be responsible for protection and preservation of the Authority's data.
3) Shall not take any ICT equipment belonging to the Authority from one department to another without a written informed consent of the respective Department/Section Head.
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.

1.8.4. The Systems Administrators/ ICT Officers 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.
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 upon written request by head of department
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 accessing or utilizing the Authority's ICT resources and specifies authorized and unauthorized use. The ICT resources can either be owned or leased by the Authority and include the following:-

i) 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.

ii) 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.

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 Authority's equipment.

2.1.3. Policy

i) NEA ICT resources shall be used for NEA 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 NEA ICT resources for unauthorized activities is against Authority's 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 Authority's ICT resources by any non-Authority users must be approved in writing by the ICT Head.

- NEA network shall not be used for the following activities;

a) The creation, dissemination, storage and display of obscene or pornographic material, hate literature, materials that promote criminal activities, defamatory materials or materials likely to cause offence to others.

b) The creation, dissemination, storage and display of any data that is illegal including, but not limited to, Statutes and Regulations of the organization.

c) The downloading, storage and disseminating of copyrighted materials including software and all forms of electronic data without the permission of the holder of the copyright.

d) Deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting the data belonging to other users.

- Unauthorized connection of monitoring devices/equipment to the NEA ICT infrastructure which could result in the violation of NEA's ICT policy, applicable licenses or contracts constitutes inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information.
- Misusing, disclosing without proper authorization, or altering information is prohibited and shall be done in adherence to the Access to Information Act no.31, 2016.
- Copyrighted material shall not be distributed, copied or published in any form without consent of the originator and any copyright violation or infringement rests solely on the user.
- NEA staff shall forfeit their rights to privacy in their use of the Internet service provided by NEA.
- The ICT department reserves the right to hardware, software and information.

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 Authority.

2.2.3 Policy

- All ICT resources acquired by the Authority under Grants/MOU/Agreements/Donation must have elaborate terms and conditions which include and specify ownership.
- All ICT resources acquired by the Authority belong to and shall remain the property of the Authority.
- 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.
- The ICT Department shall ensure all ICT resources are installed, configured, tested and commissioned as per the requirements.
- In acquisition of ICT resources, the ICT Department shall be involved in the procurement process that includes evaluation, inspection and acceptance.
- ICT and SCMD shall ensure that all ICT equipment procured by or granted to the Authority shall be identified as belonging to the Authority, GOK by tagging or engraving for identification purposes before distribution.
- The ICT Department shall use best practice and global standards and guidelines to develop technical specifications.
- At distribution, all details shall be captured into an ICT asset inventory.

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 non-staff on protection and accessibility of physical ICT resources.

3.1.3. Policy

- The Authority shall provide access control and surveillance for the ICT key installations such as server rooms, switches, cabinets and fiber channels.
- Server Rooms 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.

3.2 Guidelines

3.2.1 Access to Computer Rooms

- Only authorized staff shall work full time in computer rooms.
- Other staff and maintenance personnel shall be provided with limited access on a need-to-enter basis.
- All visitors to the computer rooms shall be escorted by an authorized staff and shall accompany the visitor until they depart.
- Computer rooms 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.

3.2.2 Access to Server Rooms

- Physical access to the server room areas must be controlled. Unauthorized persons shall not access the server rooms

- Doors to server rooms 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 server room.
- Contractors/suppliers must be accompanied by authorized officers and must enter their details in the entry/exit register.

3.2.3 Theft Prevention of Equipment

- All theft or attempted vandalism must be reported to the administration Department 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 Authority'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 server room and Computer rooms without authorization by ICT Head.

3.3. Logical security policy

3.3.1. Purpose

To enforce data integrity, confidentiality and availability.

3.3.2. Scope

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

3.3.3. Policy

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

3.3.4. 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 Authority 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 Accounting Officer
- 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 administrative 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 Authority 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.

3.4. Password policy

3.4.1. 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.

3.4.2. Scope

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

3.4.3. 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.

3.4.4. 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 Authority's 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 ninety (90) 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 eight (8) 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.
- 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 Departmental/Section Heads when a user is transferred/dismissed/retires/resigns/on leave so that their user access can be revoked.

3.5. Antivirus policy

3.5.1. Purpose

To protect the Authority'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.

3.5.2. Scope

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

3.5.3. Policy

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

3.5.4. 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 NEA 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.

3.6. Backup policy

3.6.1. Purpose

To establish the rules for the backup and storage of electronic information at the Authority. 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.

3.6.2. Scope

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

3.6.3. Policy

All Authority's systems data shall be backed up and securely stored on site and off site.

3.6.4. 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.
- 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 Authority or Department.
- Procedures between the Authority 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 source 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 Authority 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 on requirements for backup media,

3.7. Incident reporting policy

3.7.1 Purpose

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

3.7.2 Policy

All ICT related incidents shall be reported to the Head of ICT.

3.7.3 Guidelines

All security violations shall be reported as: -

- Incidents of theft, attempted theft and malicious physical damage shall be reported to 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

4.1.1. Purpose

To ensure that systems are secured from environmental exposure due to natural occurring events and to control the environment in which the systems are implemented. To also ensure that the systems do not interfere with the natural environment.

4.1.2. Scope

Applies to all the staff in the Authority and third parties**.**

4.1.3. Policy

The Authority 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 server rooms. 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 server rooms. 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 fire department** shall ensure that all fire detection systems comply with building codes. The fire department shall inspect the system and facilities annually.
- **Fireproof walls, floors and ceiling** surrounding the server rooms 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.
- **Server rooms** should have floor tiles and not carpeted to minimize dust.

4.2. Health and safety policy

4.2.1. Purpose

To ensure that staff using Authority's 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 Authority's ICT resources.

4.2.3. Policy

The Authority 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 Authority 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.

External Drives

The ICT Department 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.

System Documentation

The ICT Department shall ensure that the hard copies of systems documentation shall be physically secured in filing cabinets when not in use.

Printers, Telephone Lines, Fax, Scanners and Copiers

- NEA 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.
- 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.
- Printers will be configured to be shared by many users and placed in secured open offices where possible.
- Unofficial calls and fax will be charged on the user.
- An electronic document scanner shall be used to minimize usage of fax machines, saved in suitable formats and emailed to recipients.

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. Windows should be fitted with blinds to avoid glare for screen users.

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 hardware in the Authority.

5.1.2 Scope

The policy shall apply to all hardware in the Authority. 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 Authority.
- The use of foreign equipment in the Authority's 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 documentation.
- The ICT Department shall maintain a list of standard hardware configuration for computers that are supported by the Department 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 Authority is in compliance with applicable licenses, notices, contracts and agreements.

5.2.2 Scope

This policy applies to all software developed or acquired for the purposes of the Authority's 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 Authority will run on genuine and licensed software.
- All software acquired for or developed on behalf of the Authority shall be the property of NEA.
- All software licenses shall be managed centrally by the ICT Department.
- Source code for all application software developed for the Authority shall be the property of the Authority.

5.2.4 Guidelines

- Users shall request for software through the ICT head.
- ICT head shall maintain records of software licenses owned by the Authority
- 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.
- Authority staff shall be individually responsible for reading, understanding and following applicable licenses, notices, contracts and agreements for software usage on NEA computers. The staff shall not:
    a) Install software without authority by the ICT Department.
    b) Copy software unless authorized by the ICT Department.
    c) Download software unless authorized by the ICT Department.

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 and installation 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 NEA or leased software and data can only be released from ICT Department for non-NEA use with the written approval of the Accounting Officer.
- 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 Authority.
- ICT Department shall facilitate training on the acquired software where necessary.
- The Authority staff shall not borrow or lend any software without the consent of Head ICT.
- All software developed in house by the Authority staff shall become the property of the Authority.

Licenses

- The Authority shall comply with all laws regarding intellectual property. This applies to all software licensed or developed by ICT staff at and for the Authority.
- The Authority may negotiate for corporate licenses for 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 Authority.
- 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 Authority 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 Authority 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 Authority's customized specifications.

5.3.2 Scope

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

5.3.3 Policy

- All systems and software developed for Authority's use shall be copyrighted by the Authority on acceptance and handover of the system.
- Third party copyrighted software used by contractors engaged by the Authority as third party software shall retain copyright ownership of its original work, while at the same time granting the Authority 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 Authority '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 Authority 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 Authority.

5.4.3 Policy

- All ICT resources acquired at the Authority shall come with a written warranty.
- The Authority 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 Authority shall come with genuine licenses/warranty for a specified/agreed 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 Authority shall ensure that preventive, corrective and adaptive maintenance plan is undertaken as per GOK ICT standards.
- The Authority 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 Authority 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 Authority.
- ICT Head in liaison with SCMD shall prepare an ICT equipment maintenance contract and specification of the ICT equipment.

- ICT and SCMD shall maintain documentation and contracts on all ICT equipment maintenance undertaken by the Authority.
- Inventory of the equipment which are out of warranty shall be maintained
- Preventive maintenance shall be done on all ICT equipment at least twice a year at planned intervals.
- 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 Authority. 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 Authority with the contractor.
- The Legal Officers from the Authority 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 equipment and software, and to provide data security and confidentiality during the process.

5.7.2 Scope

This policy covers all data, ICT equipment software that are owned or operated by the Authority.

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 critical data or information is backed up and permanently erased.
- All ICT storage media shaenvll be disposed of by demagnetizing and or physically destroying them.
- All ICT equipment to be disposed of shall 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 Department shall deactivate the software system or element to prepare it for disposal.
- ICT Department shall remove the software system, its elements, its data, and non-reusable material from use or production for appropriate disposition and action.
- ICT Department shall reuse, recycle, recondition, overhaul, archive, or destroy designated software system elements.
- ICT Department shall conduct destruction of the system elements, as necessary, to reduce the amount of waste treatment or to make the waste easier to handle.

CHAPTER 6 : 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 Authority.
- All network infrastructures shall incorporate security such as firewalls, VLANs, encryptions, VPNs, intrusion detection systems and network management system.
- Core systems data being transmitted over shared/public networks shall be encrypted.

6.1.4. Guidelines

- All requests from user departments for networks such as LAN, WAN and wireless connectivity shall be made to the ICT Head for assessment and technical specifications.
- 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.
- 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 Authority's 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 documentations on network infrastructure designs, architectures, configurations and relevant manuals.

6.2. Websites

6.2.1. Purpose

To ensure that the Authority's information is provided online to the public.

6.2.2. Scope

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

6.2.3. Policy

- The Head of ICT shall coordinate the development, upgrading and maintenance of the website and ensure that it is available for access.
- It shall be the responsibility of the Department of Communications to provide authorized web content for posting into the website.
- The Head of ICT shall ensure that authorized web content from the Department of Communication is posted into the website.

6.2.4. Guidelines

- The ICT Head shall provide guidelines on the location to host the NEA's website.
- Content to be uploaded into the website shall be submitted to the Department of Communication by the respective 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 Authority.

6.3.2. Scope

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

6.3.3. Policy

Internet

- The ICT Department shall ensure that internet services are available to all members of staff.
- The Department shall put in place mechanisms to restrict access to unauthorized sites.
- Public internet access shall where applicable not be enabled on equipment providing core business applications.
- Use of internet provided by NEA (whether for personal or business purposes) may be monitored and recorded. Such monitoring will be for the purposes of NEA maintaining its security and the proper operation of the systems.
- Internet resources shall not be used for purposes which are illegal, unethical or unacceptable.
- Downloads of documents, executable file and zipped files will be subjected to malware scanning before download can commence.
- Use of the internet for non-business high volume traffic over the network which might substantially hinder other users is prohibited e.g. streaming media (audio, radio or video) or heavy software downloads.

Email

- The Authority 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 ICT Department will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill the Authority obligations to third parties.

- The official email shall not be used to send chain e-mails which may generate unnecessary high volume traffic in the hosting environment.
- User should not reply to unsolicited junk e-mails received at a NEA Email address as this could allow the sender to verify addresses for purposes of sending a virus or hacking in Authority's system.
- Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of NEA, or contain any material that is detrimental to any party outside the specific business interests of the Authority.

6.3.4. Guidelines

- Head HRM(S) shall forward names of officers who have joined/left the Authority for the purpose of creating or deleting e-mail accounts.
- Email addresses for official communication shall have the format surname.firstname@<nea>.go.ke.
- The ICT Department shall be responsible for creating the user accounts
- All NEA 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.
- NEA shall put in place a redundant link to support the primary link to GCCN network

6.3.5. 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 NEA staff and clients are accorded the necessary ICT support while using ICT resources.

7.1.2. Scope

This applies to all NEA staff and clients.

7.1.3. Policy

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

7.1.4. Guidelines

- Users shall immediately contact the ICT Department when they have ICT related problems.
- All support activities shall be logged and maintained as records as per the Department's user procedure guidelines.

7.2. Shared services policy

7.2.1. Purpose

To facilitate the sharing of resources 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

- NEA shall endeavor to identify, facilitate and consolidate all services that can be shared.
- All users shall share physical infrastructure such as network infrastructure, server rooms, 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 Authority.

7.3.3. Policy

- NEA shall create and maintain an inventory of all ICT resources which shall be updated regularly to provide the current status.
- All users leaving the Authority on retirement, dismissal or transfer shall surrender all ICT resources issued to them in line with the ICT security standards.

7.3.4. Guidelines

- All equipment and software purchased by the Authority shall remain the property of the Government of Kenya and shall be tagged appropriately.
- The ICT Department and Supply Chain Management department (SCMD) shall maintain, manage and have custody of the inventory of all ICT equipment for the Authority.
- 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 units shall be captured into the inventory.

- There shall be an ICT Equipment register to log movement of equipment to and from the Department.
- All new equipment shall be keyed into the Assets Management System.
- IT equipment shall be considered obsolete if they are damaged beyond repair or has exceed lifespan
- Obsolete ICT equipment will be disposed of as stipulated by the Public Procurement and Disposal Act of 2015.

7.4. Documentation policy

7.4.1. Purpose

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

7.4.2. Scope

The policy shall cover all documentation in the Authority 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) Systems design report

7.4.3. Policy

- The Authority 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 Accounting Officer.
- 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 Authority.

7.5.3. Policy

The Authority 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.

7.6. Project management

7.6.1. Purpose

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

7.6.2. Scope

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

7.6.3. Policy

- All ICT projects shall be implemented in line with GOK ICT Standards.
- The Accounting Officer shall constitute a project implementation committee headed by a Project Manager to oversee each ICT project.
- All ICT projects will be assigned competent Project Manager.
- NEA 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 project implementation committee
- All projects shall use a risk management framework to report all project related risks.
- All international contracted firms for the projects shall have a qualified local company that will provide support services to the project.
- After completion of each project, a formal post-project review shall be undertaken by the PIC 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 Authority on ICT skills and competencies.

8.1.2. Scope

This policy shall apply to the staff in the Authority.

8.1.3. Policy

- The Authority shall train the ICT staff in professional and industry certification courses.
- The Authority shall ensure that all ICT projects, hardware and software acquired shall have necessary training components as follows:
  - technical user training
  - professional training
  - management user training
  - operational user training
  - trainers of trainers (TOT)
- NEA 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 Authority shall ensure that all NEA staff will undergo a basic training for ICT skills.
- The Authority shall provide comprehensive training relating to the acquisition and disposal of ICT resources.
- The Authority shall provide comprehensive training 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 Authority shall facilitate training and at least one workshop annually for ICT officers to update them on emerging technologies.

- All NEA staff shall be inducted with appropriate ICT orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational goals.
- ICT staff training shall include training on management skills and priority shall be given to professional courses.
- NEA will ensure ICT staff are accredited and certified in their areas of specialization.
- The 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: PENALTIES

9.1. Penalties

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

Action will be taken in accordance with relevant Government Policies, Human Resource Policy and Procedures Manual 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:

- NEA Human Resource Policy and Procedures Manual 2019
- Public Procurement and Disposal Act of 2015.
- Ethics and Anti-Corruption Act 2003

APPENDICES

APPENDIX I: ICT POLICY COMPLIANCE AGREEMENT



NATIONAL EMPLOYMENT AUTHORITY

DEPARTMENT OF ICT

ICT POLICY COMPLIANCE AGREEMENT

I, the undersigned, have read the Authority's ICT Policy Carefully and understood the security guidelines stipulated therein. I undertake to abide by them, as I am aware that failure to abide by these guidelines may cause harm to the Authority's ICT Infrastructure and other officers sharing the same and may lead to disciplinary action being taken against me.

Name: ……..……

PF Number: ……..……

Designation: ……

Signature: ……

Date: ……

APPENDIX II: ICT EQUIPMENT MOVEMENT SAMPLE REGISTER

No.	Full Name	PF No.	Item	Serial No.	Date borrowed	Destination	Date returned	Signature
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								