REPUBLIC OF KENYA

MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY:

ICT SECURITY POLICY CONTROLS:

1. Background Information:

The Ministry has invested substantially in ICT resources. These resources are vital in realizing the Ministry's business objectives and are integral to the ability of the Ministry to operate effectively. This policy establishes general guidelines, rules and regulations for the use and protection of the Ministry's information, data, systems and utilization of ICT services.

The implementation of this Security policy will thus promote the availability, integrity and confidentiality of the Ministry's ICT systems.

2.0 Policy Objectives

The objectives of system controls and security policy are to: -

(i) Create general awareness on appropriate security measures that must be implemented to safeguard the effective operation of the Ministry;
(ii) Communicate the responsibilities for the protection of ICT systems;
(iii) Facilitate the preservation of the integrity and privacy (confidentiality) of the Ministrys' information and
(iv) Protect and promote the Ministry's reputation.
(v) Protect Ministry Data/Information against unauthorized access and utilization.
(vi) To minimize risks associated with hacking of information for malicious use.

3.0 Systems Security Control Policy

The Ministry's ICT systems, and the service they provide, will be protected by effective control of security risks at all levels of the organization, providing, managing and operating to ensure that the requirements regarding availability, confidentiality and integrity are preserved;

(i) **Access**

Access to the systems will be restricted to authorized users as determined by the head of a service area.

(ii) **Breaches**

Any breach of this policy shall be dealt with under the Ministry's Disciplinary Policy and Procedures. In addition, the Ministry may advise law enforcement agencies of the breach where it considers that a criminal offence may have been committed.

(iii) Review

The Ministry Steering Committee whose responsibilities include review of this aspect of the ICT as occasioned by changes in technology and Ministry Organisation Structure will carry out the review when necessary.

4.0 Physical Security

ICT resources are generally exposed to the risk of unauthorized access, manipulation, disruption and natural disasters. In an effort to protect the ICT equipment and systems and ensure their availability the Ministry will institute appropriate control measures to ensure that its ICT resources are safeguarded. Appropriate controls will be established to limit access to ICT infrastructure, computer equipment and data.

5.0 Passwords:

The ICT department shall prevent unauthorized access to the Ministry's corporate computer systems. Such controls shall take the form of passwords in the user identification process.

6.0 Data Security:

There shall be rules, regulations and guidelines that ensure confidentiality, integrity, availability and safety of all Ministry information.

7.0 Internet Use:

a. To ensure productive, appropriate use and to minimize risks, access to the Internet should be limited to staff who need it for their work. Users should use the Internet in an effective, ethical and in a lawful manner.

b. It is encouraged that staff use internet for critical work

c. The Ministry will occasionally audit a log of the sites visited as a means of determining appropriate usage.

d. The Ministry shall install and maintain firewalls to filter content coming in or going out via the internet and protecting external attacks.

8.0 E-mail Security:

(i) The Ministry encourages the use of email.

(ii) For proper utilization of server disk space, users are encouraged to delete Email after they have read Use of Email is permitted as long as it does not:

a. Violate this policy

b. Degrade the performance of the network and

c. Divert attention from work

(iii) Users are encouraged to use a disclaimer shall be applied to all outgoing email

9.0 Compliance

All users of the Ministry's ICT systems are required to read the ICT policy and give a written declaration that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the head of ICT.

10.0 Policy Review:

This policy will be regularly reviewed and amended as required due to technology changes and statutory regulations. The responsibility for the ongoing review resides with the head of ICT in conjunction with the Ministry Senior Management.

11.0 Policy Guidelines

A. Guidelines for Information Systems

1. Application Systems

(i) The selection of a supplier or system developer should be carried out in accordance with the existing rules and regulations on public procurement.
(ii) The duplication of copyrighted software or documentation is strictly prohibited unless for backup purposes.

2. Installation

The installation of systems will involve the following: -
(i) Preparation of end users with awareness and training prior to deployment. This is to ensure best results and to avoid unnecessary calls to user support.
(ii) Maintenance of full documentation with respect to configurations and changes. This will facilitate efficiency in management of operations, especially in the event of staff changes.
(iv) Software will be installed and rolled out only after testing.

B. Guidelines on Office Productivity Software

(i) Updates of the Office Productivity software will be carried out as and when new versions are released.

C. Guidelines on antivirus software

(i) Any new computer or laptop shall be installed with the most current antivirus software;
(ii) Any virus-infected computer must be removed from the Network until it is cleaned off the virus

D. Guidelines for Personal Computers and Servers

(i) Users are required to lodge a report of any malfunction of the computer to ICT;
(ii) Laptops should not be carried out of Ministry's buildings except for Ministry's work outside

the building. All laptops to be carried outside for external use must be recorded;

E. Guidelines on Inventory of ICT equipment

i. An annual inventory check of all ICT equipment shall be conducted.
ii. Inventory of computers shall be reviewed and updated continuously.

F. End User Training Guidelines

Ministry of Education Science and Technology employees must possess basic computer skills.

G. Systems Control and Security Guidelines

All users of the ministry's ICT systems are required to read the ICT security guidelines and give a written declaration that they will adhere to the guidelines set out in this document. The signed declaration shall be returned to Head ICT. The declaration is provided on the back page.

The ICT unit shall:

a. Ensure establishment of the ICT policy.
b. Provide support and guidance to assist users in understanding their responsibilities with regard to ICT security.
c. Grant Systems access rights.

The users of the Ministry's information systems are accountable and responsible for:

a. Understanding and adhering to this policy; and
b. Notifying any breach of ICT security to the head of ICT

1. The following system Control and security guidelines apply to all users:

a) Access to ICT equipment and systems shall be restricted to authorized users.
b) Air temperature and humidity must be controlled within acceptable limits;
c) All computer devices must be adequately protected against interruptions to electricity supply;
d) Access to the server rooms is restricted to unauthorized users
e) Air conditioning systems are functional in accordance with supplier standards.
f) All ICT equipment leaving the Ministry's premises are accompanied by a valid authorization by way of a gate pass;
g) There is consistency between the serial numbers on the equipment and the gate pass;
h) All ICT equipment that do not belong to the Ministry coming into our premises must be declared and registered
i) Users must Safeguard their workstations against damage e.g. from dust, water etc
j) ICT Unit will ensure that data stored in the Ministry Servers is backed up to prevent its loss.
k) It's a good practice that if users have to install software on their own it is done under supervision from ICT.
l) The anti-virus software should always be kept up to date.
m) Users must ensure that they do not write, distribute or introduce any software known or suspected to be infected with a virus to the Ministry's ICT systems
n) All users with access to the Ministry's ICT systems are responsible for taking appropriate

steps in selecting and securing their passwords. Users should ensure that their passwords are periodically changed. It is essential that access to ICT systems should be through the use of strong passwords.

The following rules govern the use of passwords:

i. All passwords must be changed on at most a quarterly basis;
ii. Passwords will consist of a minimum of 8 alphanumeric characters;
iii. Passwords will be kept private i.e., not shared, should not be written down and kept in secretive place;
iv. Usernames and passwords should be suspended after a specified period of disuse;
v. A user whose password has expired or account locked will be assigned an initial password by ICT and will be required to change the password immediately for security reasons.

The following rules govern the use of the Ministry's Internet access:

(a) Use of the Internet is permitted as long as it does not violate this policy and does not degrade the performance of the network and divert attention from work.

(b) Using the Internet to Solicit, Reveal or publicize Ministry's confidential information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships is prohibited;

(c) Damaging, altering, or degrading equipment providing internet and network connections thus, hindering others in their use of the Internet is also prohibited.

Users shall not:

(a) Download or store music, media or any other files where copyright issues may be of concern;

(b) Use the Ministry's Internet facility for running private businesses;

(c) Upload, download, or transmit:

1. Copyrighted materials belonging to third parties
2. Offensive, fraudulent, threatening or harassing materials

(d) Gain unauthorized access to any computing, information, or Communications devices or resources

F. Email Guidelines

(i) The following disclaimer will be applied to all outgoing email:

"This email is confidential and intended for the sole use of the individual or entity to which it was addressed. If you have received this email in error please notify the sender immediately and delete this email without disclosing, copying, using, distributing or storing its contents. Kindly note that unless expressly stated, any views or opinions presented in this email are solely those of the author and do not necessarily represent those of Ministry. The recipient should check this email and any attachments for the presence of viruses. The Ministry accepts no liability for any damage caused by this email."

(ii) Email must not be used to:

a) Send or forward emails containing defamatory, ethnic, offensive, racist or obscene remarks.
b) "Spoof" i.e. sending an email so as it appears to be from someone else.
c) "Snoop" i.e. obtaining access to the email of other people for the purpose of satisfying ones morbid curiosity

d) Attempt to breach any security measures on the email system
e) Attempt to intercept any email transmission without proper authority
f) Send “Spam” i.e. unsolicited email messages
g) Propagate viruses or generate high volume of network traffic that degrades the performance of the network.

MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY

STATE DEPARTMENT OF SCIENCVE AND TECHNOLOGY:

INTERNAL MEMO

To : Principal Secretary

Subject : ACKNOWLEDGEMENT OF ICT SECURITY POLICY

Date : 13th June, 2014

ACKNOWLEDGEMENT OF ICT SECURITY POLICY

I have read and understood the Ministry's ICT security policy.

I will adhere to the guidelines set out in this policy and understand that my contrary actions may hinder proper provision of ICT dependent services to other officers and to the public including preventing access to computer resources to which they are entitled to.

ACCEPTANCE

Name----------

PF\No. ----------

Designation: ----------

Department----------

Signature: ----------

Date: ----------