KENYA INSTITUTE OF MASS COMMUNICATION

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

DRAFT

Information and Communications Technology Policy

Kenya Institute of Mass Communication

2020

This policy was written and produced by Kenya Institute of Mass Communication
P.O. Box Kenya 42422
Telephone:
Email: info@kimc.ac.ke
Website: www.kimc.ac.ke

POLICY TITLE: Information, Communications and Technology Policy

POLICY THEME: Provisision of data that is securely accessed, stored and transmitted by shared responsibilities.

POLICY CONTACT: HOICT

APPROVAL AUTHORITY: DIRECTOR

CATEGORY: ICT services and Automation

<u>SIGNED</u>

TABLE OF CONTENTS

PREAMBLE

The Kenya Institute of Mass Communication vision and mission is to become a center of excellence in technical and professional mass media training in the region and to train high quality technical and mass media personnel to serve in both local and international media and communication industry respectively. In achieving the vision and mission, information and Communications technology is of paramount importance.
The Information Communication and Technology Committee (ICTC) on behalf of the institute has developed a blueprint that will act as a guide in the effective use of ICT resources in the Institute.

ACKNOWLEDGEMENT

The Kenya Institute of mass communication ICT Policy has evolved from a consultative process .The ICT Security Standards are modeled around best practice IT Security Standards and Guidelines in the private and public sector including those developed by institutions worldwide.

LIST OF ABBREVIATIONS AND ACRONYMS

KIMC –Kenya Institute of Mass Communication.

OS- Operating system

CPU-Central Processing Unit

End user – Person that a software program or hardware device is designed for.

CD-ROM- Compact Disc Read-Only Memory

CD: Compact disc

ICT: information and communications technology

LAN: Local Area Network

PC: Personal Computer

HICT: Head of information Communications and Technology

STATEMENT OF PURPOSE

The purpose of this ICT Policy is to outline the acceptable use guidelines for ICT equipment and services at the Kenya Institute Mass Communication. These are general guidelines on what can be done, and what should not be done, on the Institute's ICT Infrastructure in order to ensure efficient and effective use of Institute's ICT resources; protect ICT resources from injurious actions, including virus attacks, data loss, unauthorized access, network and system failures, and legal problems.

1. ICT SECURITY

1.1 Policy Statement

KIMC acknowledges its responsibility to ensure appropriate security for all data, equipment, and processes in its domain of ownership and control. This policy intends to promote a culture of openness, trust and integrity

1.2 Definition of ICT Security

ICT security is defined as "protecting information and communications systems from unauthorized acces disclosure, disruption, modification, or destruction" to ensure confidentiality, Integrity, efficiency and availability.

The assets that must be protected include:

a) Computers, Servers and Peripheral equipments
b) Application computer programs and documentation
c) Information
d) Data storage media
e) Studio equipments
f) Filming equipments

Efficient and Approriate Use ensures that the institute's ICT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

Availability is concerned with the full functionality of a system (e.g. human resource or payroll) and its components.

Confidentiality refers to the privacy of personal or corporate information. This includes issues of copyright.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disk fails, or subtle, as when a character in a file is altered

The potential causes of these losses are termed as "threats". These threats may be human or non-human, natural, accidental or deliberate.

1.3 Roles

1.3.1 Policy management

Approval of the ICT Policy is vested with the Director.

Advice and opinion on the draft Policy is given by:

a) Management Board
b) Academic Board
c) HICT

1.3.2 Implementation

Implementation and maintenance of the policy is the responsibility of Head of ICT Department.

Members of KIMC staff and students are responsible for meeting all ICT standards, guidelines, codes of practice(s) and conditions as stated in this policy.

ICT Security of each system will be the responsibility of its custodian

1.3.3 Custodian

Custodian refers to any persons, Unit or Department with the responsibility for the management or operation of any one or a combination of the following: ICT equipment,software or system in particular:

a) The ICT department is the custodian of all strategic computer platforms.
b) The ICT department is the custodian of all communications systems.
c) The ICT department is custodian of all strategic applications such as the school management system, computer application softwares and operating systems.
d) Offices, departments and individuals are responsible for the desktop system or laptops under their control;
e) The Registrar/Dean/Head of Training department/Head of Department is the custodian of any information considered confidential to the department e.g. examination results etc
d) Other strategic applications will be managed by the designated custodian

1.3.4 Domains of Security

This policy deals with the following domains of security:

a) Computer System Security: CPU, Peripherals, OS, including data security.
b) Physical Security: The premises occupied by the ICT personnel and equipment

1.3.5 Institute's Services

Departments at the institute provide services that relate to ICT security both directly and indirectly. It is expected that there will be collaboration between these departments and the ICT Department in the development of standards and implementation of the policy.These departments are:

a) Human Resource: Personnel selection, induction, and exit-processing, Payroll.
b) Academic Registrar: Policies concerning confidentiality, privacy, information integrity.
c) Training departments: Policies concerning confidentiality, privacy, information integrity.
d) Finance Office: Policies concerning confidentiality, privacy, information integrity transactions, balance sheets, reports.
e) Audit office: Policies concerning confidentiality, privacy, information integrity.
f) Clinic: Policies concerning confidentiality, privacy, information integrity.
g) Maintenance services: Overall maintenance

1.3. 6 Standards and Guidelines

Standards (mandatory) and guidelines (suggestions) are published with this policy to assist ordinary end-users and system custodians meet their ICT security responsibilities. These standards and guidelines are an integral part of this Institute's ICT Policy and therefore define it in detail.

2. ACCESS TO ICT FACILITIES

a) All communications rooms and cabinets shall be locked at all times.
b) Entry to communications rooms and cabinets, and interference with ICT network equipment is strictly prohibited.
c) Other than in an emergency, access to communications rooms, cabinets and ICT network equipment shall be restricted to designated members of staff of the ICT department.
d) Contractors providing ICT network services must obtain the prior approval of the Head of ICT and shall obtain the appropriate authorization in compliance with procedures and regulations of the Institute's security system.

3. ACCESS IN AN EMERGENCY

a) In the event of a fire or other emergency, security staff and/or staff Maintenance Department and/or the emergency services may enter these areas, without permission, to deal with the incident.

b) Where ICT network equipment is housed in rooms used for other purposes, the arrangements for access by the other user of the room shall require prior written consent of the Head of ICT. This consent shall specifically exclude access by the other user to any communications cabinets or ICT network equipment located in the shared room.

4. CONDITIONS OF USE OF COMPUTING AND NETWORK FACILITIES

a) It is the policy of the Institute that the computing and network facilities are intended for use for teaching, learning, research, administration and management in support of the Institute's mission. While recognizing the increasing importance of these facilities to the activities of staff and students, the Institute reserves the right to limit, restrict, or extend access to them.

b) All persons using the computing and network facilities shall be responsible for the appropriate use of the facilities provided as specified by the "Codes of Practice" of this policy, and shall observe conditions and times of usage as published by the ICT department from time to time.

c) It is the policy of the Institute that the computing and associated network facilities are not to be used for commercial purposes or non-Institute's-related activities without written authorization from the Institute. In any dispute as to whether work carried out on the computing and networking facilities is internal work, the decision of Director or the management board shall be final.

d) The end-users will not record or process information which knowingly infringes any patent or breaches any copyright.

e) The Institute will endeavour to protect the confidentiality of information and material furnished by the user and will instruct all computing personnel to protect the confidentiality of such information and material, but the Institute shall be under no liability in the event of any improper disclosure.

f) The Institute will endeavour to safeguard the possibility of loss of information within the Institute's computing and network facilities but will not be liable to the user in the event of any such loss. The end-user must take all reasonable measures to further safeguard against any loss of information within the Institute's computing and network facilities.

g) If a loss of information within the system can be shown to be due to negligence on the part of the computing or network personnel employed by the institute, or to any hardware or software failure which is beyond the end-user's means to avoid or control, then the ICT department will endeavour to help restore the information.

h) The use of the computing and network facilities is permitted by the Institute on the condition that it will not involve the infringement of any patent or the breach of any copyright.

i) End-users of the computing and network facilities recognize that when they cease to be formally associated with the institute (e.g. no longer an employee or enrolled student), they cease to be authorized users and access to the said facilities will be denied. Inaddition, their private information may be removed from institute's computing and network facilities without notice.

j) The Institute reserves the right to limit permanently or restrict any end-user's usage of the computing and network facilities: to copy, remove or delete, or otherwise alter any information or system that may undermine the authorized use of the computing and network facilities; and to do so with or without notice to the user in order to protect the integrity of the computing and network facilities unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

k) The Institute, through authorized individuals, reserves the right to periodically check and monitor the computing and network facilities, and reserves any other rights necessary to protect them.

l) The Institute disclaims responsibility and will not be responsible for loss or disclosure of user information or interference with user information resulting from ICT department's efforts to maintain the privacy, security and integrity of the computing and networking facilities and information.

m) The Institute reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive the rights of the institute to take additional actions under this policy.

n) The ICT department may disable or disconnect any person from using the computing and networking facilities (and may recommend additional penalties to the management board/academic board and the Director) if after appropriate investigation that person is found to be:-

i. Responsible for wilful physical damage to any of the computing and network facilities;
ii. In possession of confidential information obtained improperly;
iii. Responsible for wilful destruction of information;
iv. Responsible for deliberate interruption of normal services provided by the ICT department;
v. Gaining or attempting to gain unauthorized access to accounts and passwords;
vi. Gaining or attempting to gain access to restricted areas without authority;
vii. Responsible for inappropriate use of the facilities;

o) Use of the computing and networking facilities which would prevent Institute's users from having their usual access to the facilities shall not be undertaken.

5. CODE OF PRACTICE IN THE USE OF COMPUTING AND NETWORK FACILITIES

5.1 Introduction

Standards for the use of the Institute's computing and network facilities derive directly from standards of common sense, self respect and common decency that apply to the use of any shared resource.

The institute's code of practice has been published under the spirit of mutual respect and cooperation

5.1.1 Appropriate or Acceptable use

Appropriate and responsible use of the Institute's computing and networking facilities is defined as use that is consistent with the teaching, learning, research, administrative and management objectives of the Institute's and with the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use.

5.1.2 Responsibilities

End-users of the Institute's computing and networking facilities accept the following specific responsibilities;

i. **Security;**
   a) To safeguard their data, personal information, passwords and authorization codes, and confidential data;
   b) To take full advantage of file security mechanisms built into the computing systems;
   c) To choose their passwords wisely and to change them periodically; and
   d) To follow the security policies and procedures established.

ii. **Confidetiality**
   a) To respect the privacy of other users; for example, not to intentionally seek information on, obtain copies of, or modify files, CD-ROMs, or passwords belonging to other users or the Institute;
   b) Not to divulge sensitive personal data to which they have access concerning staff or students without explicit authorization to do so.

iii. To respect the legal protection provided by copyright and licensing of programs and data; for example, not to make copies of a licensed computer program to avoid paying additional license fees to share it with other users.

iv. To respect the intended usage of systems, for example, not to send forged electronic mail, mail that will intimidate or harass other users, chain messages that can interfere with the efficiency of the system, or promotional mail for profit-making purposes. Also, not to break into another user's electronic mailbox or read someone else's electronic mail without their permission.

v. To respect the integrity of the computing and network facilities; for example, not to intentionally develop or use programs, transactions, data, or processes that harass other users or infiltrate the system or damage or alter the software or data components of a system. Alterations to any system or network software or data component are to be made only under specific instructions from authorized ICT-Department staff, academic staff, department and unit heads, project directors, or management Staff.

vi. To report any information concerning instances in which the Institute’s ICT Policy or any of ICT Department standards and codes of practice has been or is being violated to the ICT helpdesk.

6. INFORMATION ETHICS FOR SPECIFIED ACTIVITIES.

The following apply to specific activities;

6.1 *Illegal Activity*

It is considered the inappropriate use to store and/or give access to information on the Institute computing and network facilities that could result in legal action against the Institute.

6.2 Objectionable material

The Institute’s computing and network facilities must not be used for the transmission, obtaining possession, demonstration, advertisement or requesting the transmission of objectionable material namely:

a) **An article that promotes crime or violence, or incites or instructs in matters of crime or violence; or**

6.3 Restricted Hardware or Software

End-users should not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other Information which could result in the violation of any of the Institute’s policy or the violation of any applicable license or contract.

This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers.

The unauthorized physical connection of monitoring devices to the computing and network facilities which Could result in the violation of Institue’s policy or applicable licenses or contracts is inappropriate use.

This includes but is not limited to the attachment of any electronic device to the computing and network facilities for the purpose of monitoring data, packets, signals or other information.

Authorization to possess and use such hardware for legitimate diagnostic purposes must be obtained from the head of ICT.

6.4 Copying and copyrights

a) Users of the computing and networking facilities must abide by the Copyright laws of Kenya as provided for in the Copyright Act.

b) Respect for intellectual labour and creativity is essential to academic discourse. This tenet applies to works of all authors and publishers in all media. It includes respect for the right to acknowledgment and right to determine the form, manner, and terms of publication and distribution. If copyright exists, as in most situations, it includes the right to determine whether the work may be reproduced at all.

c) Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the computing and networking facilities or for distribution outside the Institute

6.5 **Game playing**

a) Institute's computing and network services are not to be used for extensive or competitive recreational game playing.

6.6 Commercial Use

a) Institute's computing and network facilities are provided by the Institute for the support of the Institute's mission. It is inappropriate to use the computing and network facilities for:

   i. Commercial gain or placing a third party in a position of commercial advantage

   ii. Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the mission of the Institute or the service being provided.

6.7 Use for Personal Business

The Institute's computing and network facilities may not be used in connection with compensated outside work or for the benefit of organizations not related to the Institute, except in connection with scholarly pursuits such as external examination, assessment or academic publishing activities.

6.8 Connection to the network

Buildings at the Institute are included in LAN. To maintain the integrity of the Institute computing and network facilities, connections to the Institute network are made only by specialized personnel under the direction of the

ICT Department. All requests for additional network connections or for the relocation of a connection should be directed to the ICT Department.

6.9 Use of desktops

End-users are responsible for the security and integrity of Institute's information stored on their personal desktop system from wherever they are working. This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing required operating system patches and using appropriate virus protection software.

End-users should avoid storing passwords or other information that can be used to gain access to other Institute's computing resources.

End-users should not store Institute's passwords or any other confidential data or information on their laptop or home PC or associated floppy disks or CD's, or flash disks.

6.10 Use of External services.

Networks and telecommunications services and administrative systems and services to which the Institute maintains connections have established acceptable use standards. It is the end user's responsibility to adhere to the standards of such networks. The Institute cannot and will not extend any protection to users should they violate the policies of an external network.

6.10 Print outs.

Users are responsible for the security and privacy of printouts of the Institute's information.

7. APPROPRIATE USE OF ELECTONIC MAIL

7.1 Statement

Electronic mail and communications facilities provided by the Institute are intended for teaching, learning, research, outreach and administrative purposes. Their use is governed by Institute's rules and policies and acceptable Use Policy of the provider. Electronic mail may be used for personal communications within appropriate limits.

7.2 Approriate use and Responsibility of Users.

Users should explicitly recognize their responsibility for the content, dissemination and management of the messages they send. End users should ensure that emails sent through the Institute's network should adhere to the following;

i. Do not contain information that is harmful to the Institute or members of the University community;
ii. Are consistent with Institute's policies;
iii. Protect others' right to privacy and confidentiality
iv. Do not contain obscene, offensive or slanderous material;
v. Are not used for purposes that conflict with the Institute's interests;
vi. Do not unnecessarily or frivolously overload the email system (e.g. spamming and junk mail are not allowed); and
vii. Are not for commercial purposes unless authorized by the Institute.

7.3 Data backups

It is the responsibility of the individual user to backup their own data from their computers, safely onto CD, or other storage media.

7.4 Confidentiality and Security

i) As Institute's networks and computers are the property of the Institute, the Institute retains the right to allow authorized Institute's officers to monitor and examine the information stored within.
ii) It is recommended that personal confidential material not be stored on or sent through Institute's equipment.
iii) End-users must ensure the integrity of their password and abide by Institute guidelines on Passwords.
iv) Sensitive confidential material should NOT be sent through the electronic mail system unless it is encrypted.
v) End-Users should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies

7.5 User Indemnity

Users agree to indemnify the Institute for any loss or damage arising out of improper use.

7.6 Limited Warranty

The Institute takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages or data nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

8. *GUIDELINES ON PASSWORDS*

8.1 Password Management

i) Passwords should be memorized - **never** written down.

ii) Passwords belong to individuals and must **never** be shared with anyone else.

iii) Passwords should be changed regularly at intervals of not more than three months, or immediately if compromised

8.2 Password Construction

i. A password should be at least 6 characters long.

ii. Never make your password a name or something familiar, like your pet, your children, or partner.

iii. Never, under any circumstances, should your password be the same as your username or your real name.

iv . End users should not use words that are associated with them.

8.3 Password Management

i) Passwords should be memorized - **never** written down.

ii) Passwords belong to individuals and must **never** be shared with anyone else.

iii) Passwords should be changed regularly at intervals of not more than three months, or Immediately if compromised

8.4 Password Construction

i. A password should be at least 6 characters long.

ii. Never make your password a name or something familiar, like your pet, your children, or partner.

iii. Never, under any circumstances, should your password be the same as your username or your real name.

iv. End users should not use words that are associated with them.

9. STUDENT LABORATORY CODE OF PRACTICE

9.1 Introduction

The “Student Laboratory and Network Code of Practice” is applicable to all student users, Institute staff and any other users authorised to access the student laboratories and network. Access to the computer Laboratory is provided by the Institute for academic, research or study purposes only. It the end user's obligation to use the facilities in an efficient, ethical, legal and responsible manner, in accordance with the Institute's "Code of Practice in the Use of Computing and Network Facilities", "Appropriate Use of Electronic Mail", and the code of conduct specified below.

9.2 Identification

Computer Labs are provided for Institute students and staff.

9.3General Configuration Requirements

i. Computer laboratories shall be prohibited from engaging in port scanning, network auto discovery, traffic spamming or flooding, and similar activities that may negatively impact on the overall health of the Institute's network.

ii. In computer laboratories where non-Institute's users are allowed access (such as computer training laboratories), direct connectivity to the Institute's data from such laboratories shall be prohibited. In addition, no Institute's confidential information shall reside on any computing equipment located in such laboratories.

9.4 Illegal activities

i. Do not download or copy software without appropriate authority or license.
ii. It is an offence to knowingly inject viruses into any system or engage in any other form of hacking.
iii. It is an offence to transmit material which is offensive, obscene, harassing, slanderous, damaging to the files or programs of others, or which violate any applicable law.
iv. The ICT department reserves the right to interrupt laboratory connections if such connections are viewed to impact negatively on the ICT infrastructure, or pose a security risk.

9.5 Laboratory Etiquette

i) No food, drink or cigarettes are to be consumed in the laboratories
iii. Avoid excessive noise
iv. Game-playing is not desirable. It is forbidden.
v. You are required to comply with any instruction by the Institute's lab assistant or security officer

10. INTERNET CONDITIONS,STANDARDS AND GUIDELINES

10.1 Introduction

The Internet introduces new opportunities and new risks. In response to the risks, this statement describes the Institute's official policy regarding Internet security. It applies to all Institute's employees, students,contractors, and temporary staff who use the Internet with Institute computing or networking resources.

10.2 Transmission of Information

i. Downloading

All software downloaded from non-Institute sources via the Internet must be screened with virus detection software prior to being invoked

ii. Contacts

Contacts made over the Internet should not be trusted with Institute's information unless reasonable steps have been taken to ensure the legitimacy of the contacts. This applies to the release of any internal Institute information.

iii. Information Security

Log-in passwords, and other parameters that can be used to gain access to Institute systems, networks and services, must not be sent over the Internet readable form.

iv. Software security

Institute's computer software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Institute party for any purposes other than Institute purposes.This will be expressely authorized by heads of departments and ICT department.

Exchanges of software and/or data between the Institute and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

10.3 Bring You Own Device(BYOD)

i. Employees who prefer to use their personally-owned IT equipment for work purposes must secure Institute's data to the same extent as on the Institute's ICT equipment, and must not introduce unacceptable risks (such as malware) onto the Institute's networks by failing to secure their own equipment.

ii. BYOD users must use appropriate forms of user authentication approved by Information Security, such as user IDs, passwords and authentication devices.

iii. The following classes or types of Institute data are not suitable for **BYOD;**

a) Anything classified SECRET or CONFIDENTIAL;

b) Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as SECRET or above;

iv. The Institute has the right to seize and forensically examine any device within the In premises believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

v. Device users must ensure that valuable Institute's data created or modified on the devices are backed up regularly.

vi. While employees have a reasonable expectation of privacy over their personal information on their own equipment, the Institute has right to control its data and manage devices may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, device users are advised to keep their personal data separate from Institute data on the device in separate directories, clearly named (e.g. "Private" and "BYOD").

11. STRATEGIC INFORMATION SYSTEM PLATFORMS

11.1 Definition

A strategic system may be defined as a system that meets *several* of the following criteria:

i. Is critical to the mission of the Institute ;
ii. Affects large parts of the Institute;
iii. Yields Institute's-wide benefits;

11.2 Physical security

The following standards of physical security of strategic platforms must be met:

i. Premises must be physically strong and free from unacceptable risk from flooding, vibration and dust
ii. Air temperature and humidity must be controlled to within acceptable limits
iii. Platforms must be electrically powered via UPS to provide the following:
   a) Minimum of 15 minutes' continuous operation in the event of a power blackout;
   b) Adequate protection from surges and sags; and trigger an orderly system shutdown when deemed necessary.

11.3 Physical Access

i) Premises will be staffed and controlled by designated ICT department staff.
ii) External doors will remain locked, preferably with electronic locks and or grilled doors.

11.4 User access

i. New Users

New user-ids will be handled as follows;

a) Written application must be submitted on an official form;
b) The application form must be signed by someone in authority (e.g. **HR,HOD**);
c) The applicant must present suitable personal identification
d) The application form will be kept indefinitely by ICT-department
e) The new userid and password will be given orally to the applicant
f) The password must be set to force password change on the first login
g) The access level will be no higher than required as approved by the custodian.

ii. Terminating Users

The user-ids of persons leaving the Institute or no longer requiring access will be disabled.

11.5 Data Integrity

a) Security backups of all data will be made daily

b) The backup regime must meet the following criteria:

i) Enable recovery to at least the start of business on any weekday of a failure.

ii) Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.

iii.) There must be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.

c.) There must be a validation of security backup media at least once every six months.

11.6 Password Aging

The life of a password should be no more than 3 months.

11.7 Disaster Recovery Plan

There will be a Disaster Recovery Plan for every Strategic system.

11.8 Business Continuity

There should be a Business Continuity evaluation along the following lines:

i. A determination of the maximum time of not having the service(s) provided by the system that can be tolerated. This will be determined by the ICT department having carried out an evaluation of the relevant systems.

ii An identification of all of the threats to the system such as:

a) Hardware Failure;
b) Electrical Power Failure
c) Fire.

12. DESKTOP/LAPTOP COMPUTER SECURITY GUIDELINES

12.1 Introduction

Desktop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units.

12.2 General Obligations

Users and custodians of desktop computers are subject to the "Conditions of Use" and "Code of Practice" specified in the Institutes's ICT Policy.

12.3 Hardware Security

The following guidelines apply;

i. Lock offices. Office keys should be registered and monitored to ensure they are returned when the owner leaves the Institute;

ii. Secure hard disks. External hard disks should be secured against access, tampering, or removal

iii. Mark departmental computers clearly with the access control numbers of the Institute.

iv. Locate computers away from environmental hazards

v. Store critical data backup media in fireproof vaults or in another building; and

vi. Register all Institute's computers.

12.4 Access Security

Utilize password facilities to ensure that only authorized users can access the system

Password guideline:

a) should be eight characters

b) Avoid words found in the dictionary and include at least one numeric character. (Six-character passwords may suffice for non-dictionary words.) ;

c) Choose passwords not easily guessed by someone acquainted with the user. (For example, passwords

d) Should not be maiden names, or names of children, spouses, or pets.) ;

e) Do not write passwords down anywhere

f) Change passwords periodically; and

g) Do not include passwords in any electronic mail message.

12.5 Data and Software Availability

a) Back up and store important records and programs on a regular schedule

b) Check data and software integrity

12.6 Confidential Information.

a) Monitor printers used to produce sensitive and confidential information.

b) Overwrite sensitive files on fixed storage media.

12.7 Software

Licences of software vendors should be complied with. The institute may not be subject to random license audits by software vendors.

12.8 Computer networks at the Institute

While the ICT Department has responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment.

The following considerations and procedures must be emphasized in a network environment

a) Check all files downloaded from the Internet. Avoid downloading shareware files.
b) Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers.
c) Always **back up** your important files.
d) Test all software before it is installed to make sure it does not contain a virus/worm that could have serious consequences for other personal computers and servers on the Institutes networks.

12.9 Communications network management

The Institute's Communications Network is comprised of communications infrastructure, equipment, and standards associated with the transport of data and telephony throughout the Institute.

The ICT Department will be responsible for the overall management of the Communications Network, managing and administering appropriate standards to ensure consistency and quality of communications services.

12.10 Service levels

12.10.1 Accessibility

a) All staff and students where appropriate, will be provided with access to voice and data services.
b) Helpdesk and telecommunication support services will be provided by ICT Department.

12.10.2 Reliability

The Communications Network will be designed to be available as close as possible to 100% of the time, 24 hours a day, seven days a week.

12.10.3 Security

The Communications Network equipment and infrastructure will be physically secured against internal and external security threats.

13. ICT EQUIPMENT DISPOSAL

The Institutes surplus or obsolete ICT equipment (i.e. desktop computers, servers, etc.) must be disposed of according to legal requirements and environmental regulations through appropriate external agents and Institute's upgrade guidelines.

13.1 Guidelines

Disposal of surplus ICT equipment (that are assets) will follow existing policy associated with the disposal of the equipment.

13.2 Practices

Before equipment is considered for disposal, it is recommended that the owner or requester contact the ICT Department to determine if the equipment could be re-used in the Institute as per the Primary and Secondary deployment guideline.

14. COMPUTERS AND RELATED ACCESSORIES PROCUREMENT

14.1 Purchase of Computers and related equipment

The ICT-Department will approve all specifications for servers, workstations, PCs and related equipment purchased by the Institute's Procurement Office in accordance with the Public Procurement and Disposal Act (2005).

14.2 Computer warranty

All PCs carry a warranty as a standard. The minimum warranty is at least one year.

11.9 Documentation

Procedures reflecting these policies must be documented by the ICT-Department

.