JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

December 2013

Jaramogi Oginga Odinga University of Science and Technology

Information and Communications Policy

2013

© Copyright JOOUST 2013

This policy was written and produced by Jaramogi Oginga Odinga University of Science and Technology

P.O. Box 210-40601 Bondo, Kenya

Telephone: + 254 - 57 2501804 / 2058000

Fax: + 254 - 572523851

Email: vc@jooust.ac.ke

Website: http://www.joust.ac.ke

Policy Title:	Information and Communications Technology (ICT) Policy
Policy Theme:	Provision of quality computer-based information to authorised users; securely accessed, stored, processed and transmitted at all times and underpinned by shared responsibilities.
Policy Contact:	Director, ICT
Approval Authority:	The Council
Category:	ICT Services and Automation
Reference No:	JOOUST/VC/LO/P/002
Status:	Approved by Council 20th December 2013. Minute: 8/05/12/13
Commencement Date:	20thDecember 2013
Signed:	

_____   24th Jan 2014
Vice-Chancellor, Secretary to Council   **Date**
Prof. S. G. Agong'

_____   24th Jan. 2014
Chairman of Council   **Date**
Dr. B. J. Mwandotto

TABLE OF CONTENTS

PREAMBLE

Jaramogi Oginga Odinga University of Science and Technology (JOOUST) was established by the Government of Kenya as the successor to Bondo University College (BUC) through the Jaramogi Oginga Odinga University of Science and Technology Charter 2013

JOOUST currently has 300 computers for various end-users, and three high end servers for strategic application platforms such as Financial and Student Information subsystems. All computers have power conditioning supported by a 500 KVA generator and dedicated un-interruptible power supply. At its inception in May 2009 the only ICT equipment BUC had at its disposal were 5 desktop computers inherited from Maseno University. Internet connectivity to BUC was solely through broadband MODEMS which was slow and expensive since not even a single Broadband operator Orange, Safaricom, Zain and YU could offer 3G speeds in the region.

LAN: In October 2010, a comprehensive IT infrastructure development plan for LAN, PABX system, trunking and cabling was developed by the ICT-Directorate. All the civil works, trunking and cabling was done in-house save for fibre optic splicing outsourced due to the specialized equipment required. The star bus system has been successfully rolled out to all existing buildings in phases. Provisions are made to connect to the new University Laboratory Complex and Library when they are handed over.

Internet Connectivity: The initial installation of the 2 MB internet connection by Telkom was commissioned on 1st April 2011. It involved trenching and laying of both fibre optic and copper cables from the Telekom exchange in Bondo town to the main campus, a distance of 2.7 Kms.

This last mile cable was intended to tap into the already existing Telkom High speed radio network whose nearest point of presence is at the Bondo Telkom Exchange. Apart from data, this radio also serves voice subscribers. The initial 2MB internet bandwidth was increased to 6Mbps in October 2011 and further to 10Mbps in April 2013.

The high speed radio link circuit runs from Bondo Town via Siaya Town, Samia hills, Maragoli Hills and finally joins at Kisumu the main Telkom owned national fibre backbone to Nairobi terminating at Jambonet, a section of Telkom concerned with bandwidth distribution. The only bottleneck to extra bandwidth for JOOUST on the radio link so far is at Bondo Exchange with a Radio unit of limited capacity. This is however upgradable. Otherwise, the rest of the sections of this link have enough capacity for bandwidth in excess of 378 Mbps.

From Kisumu City, Telkom's backbone to its main Network Operations Centre (NOC) at Jambonet Nairobi is primarily via proprietary fibre network. Redunancy is provided by 3 other high speed links which converge at Telekom offices at Communication Commission of Kenya (CCK)'s Mt. Longonot base station and proceed to Jambonet. From Jambonet, connectivity to the rest of the world is through The East African Marine System (TEAMS) fibre via KPLC's fibre and NOFBI (between Nairobi and TEAMS Mombasa Terminal point). Telkom has an additional international connection, a 3,000 km-long LION2 cable which extends the Lower Indian Ocean Network (LION) submarine communications cable system that connects Madagascar, Réunion, and Mauritius.

In July 2013 a Wi-Fi network exclusively for students campus wide access to the Internet (6MB) and independent of the fixed LAN was installed. Internet connectivity for the Wi-Fi is delivered via a dedicated high speed radio link.

Connectivity Services: The internet connection is currently used for general web browsing and e-mail. Email access, however is open to both JOOUST's corporate e-mail users as well as free web based e-mails such asYahoo, Gmail, Hotmail and so on. Since its elevation to a full fledge University Status, the JOOUST''s website has been re-built and is live at http://www.jooust.ac.ke

In order to utilize the, Integrated Services Digital Network (ISDN) functionality of the already existing Telkom Kenya's connectivity a PABX system, Panasonic TDA 200 a hybrid IPX, which can be configured to meet the present needs and expand has been commissioned. It combines PABX reliability with IP technology and allows plug in of GSM modules and additional cards and telephones. The phased roll out of the telephone network across the main campus is complete.

Governance: The JOOUST Statutes 2013 in particular Statute XXXVII establishes an ICT Board Chaired by the Deputy Vice-Chancellor (PAF) with the Director, ICT as secretary.

Academic Programmes Support: To date at the main campus there are two(2) computer labs of 40 PCs each, a lab of 10 computers dedicated for GIS training, 3 LCD projectors; a smart board system; the library houses 20 Internet enabled PCs; all administrative offices have Internet connection and printing is vide print servers strategically placed, and Kisumu Learning Centre (KSL) has a lab of 20 PCs. The Library has subscribed to e-resources accessible to users on both campuses.

Most undergraduate Education programmes have IT units comprising one-third of total units serviced by the School of Informatics and Innovative Systems (SIIS). A suite of postgraduate MSc and undergraduate BSc programmes in Computer Science, Information Systems, IT and Computer Security and Forensics as well as specialized Diploma courses have also been mounted.

IMIS: The University is currently implementing a strategy for a University-wide Integrated Management Information System (IMIS), whose generic sub systems will be Finance and Accounting, Student, Staff, Services, and Resources.. The phasing is based on management priorities, cost effectiveness and user department/division e-readiness. Combinations of outsourced, in house developed and customized sub systems/modules are being considered. The first phase is the implementation of the Financial subsystem including Student finance.

ACKNOWLEDGEMENT

Jaramogi Oginga Odinga University of Science and Technology ICT Policy has evolved from a consultative process involving key stakeholders at the University including the Vice Chancellor, the Deputy Vice Chancellors, Registrars, Finance Officer, Deans of Schools, Directors of Institutes, Heads of Department, lecturers and students.

The ICT Security Standards are modeled around best practice IT Security Standards and Guidelines in the private and public sector including those developed by Universities worldwide.

LIST OF ABBREVIATIONS AND ACRONYMS

CAT	Continuous Assessment Test
CCK	Communications Commission of Kenya
FTP	File Transfer Protocol
ICT	Information and Communications Technology
ITU	International Telecommunication Union
JOOUST	Jaramogi Oginga Odinga University of Science and Technology
LMS	Learning Management System
MIS	Management Information System
ODEL	Open, Distance and Electronic Learning
PAF	Planning, Administration and Finance
RIO	Research, Innovation and Outreach
ROI	Return on Investment
SCORM	Shareable Content Object Reference Model
UPS	Unlimited Power Supply
VLE	Virtual Learning Environment
WAN	Wide Area Networks

1 ICT SECURITY

1.1 Policy Statement

Jaramogi Oginga Odinga University of Science and Technology acknowledges its responsibility to ensure appropriate security for all data, equipment, and processes in its domain of ownership and control. However, this obligation does not necessarily mean a guarantee of confidentiality of the same. The University shares this obligation with every member of the university community.

1.2 Definition of ICT Security

ICT security is defined as "protecting information and communications systems from unauthorized access, use, disclosure, disruption, modification, or destruction". The risks involved here concern:

a) Confidentiality of information
b) Integrity of data
c) Assets
d) Efficient and appropriate Use
e) System availability

The assets that must be protected include:

a) Computers, Servers and Peripheral Equipment
b) Communications Equipment
c) Computing and Communications Premises
d) Data Storage Media
e) System Computer Programs and Documentation.
f) Application Computer Programs and Documentation
g) Information

Efficient and Appropriate Use ensures that University 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 disc fails, or subtle, as when a character in a file is altered.

The potential causes of these losses are termed "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 University Council.
 Advice and opinion on the draft Policy is given by:
      a) The Senate
      b) The Management Board

c) The Directorate of Information and Communication Technology

1.3.2 Implementation

Implementation and maintenance of the policy is the responsibility of the Director, Directorate of Information and Communications Technology (ICT) herein referred to as ICT-Directorate.

Members of university 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' will refer to any persons, Unit or Department or School or Institute or Centre or Division 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-Directorate is the custodian of all strategic computer platforms;
b) The ICT-Directorate is the custodian of all communications systems;
c) The ICT-Directorate is custodian of all strategic applications such as the Integrated Management Information Systems (IMIS);
d) Offices, Units and individuals are responsible for the desktop system or laptops under their control;
e) The Dean/Director of School/Institute/Centre and Head of Division/Department is the custodian of any information considered confidential to the unit e.g. examination results, financial data etc..;
f) Other strategic applications will be managed by the designated custodian.

1.3.4 Domains of Security

This policy will deal 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.
c) Operational security: Environment control, power equipment, operation activities.
d) Procedural security by ICT vendor, management and procurement liaison personnel**,** as well as ordinary users.
e) Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

1.3.5 University Services

It is recognized that various departments of the University 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-Directorate in the development of standards and implementation of the policy. Some of these sections and their services are:

a) Human Resources: Personnel selection, induction, and exit-processing
b) Registrars: Policies concerning confidentiality, privacy, information integrity and copyright
c) Finance Office :Policies concerning concerning confidentiality, privacy, information integrity i.e. Payroll , transactions, balance sheets, reports
d) Central Services: Physical building security

1.3.6 The Role of the ICT-Directorate

The ICT-Directorate, will be headed by the Director ICT who will be answerable to the Vice-Chancellor. The Directorate will develop the capacity to support the university in the following ways:

a) Improve teaching and learning through use of Innovative Learning Technologies (ILTs)
b) Provide infrastructural support for Virtual Learning Environments (VLEs)
c) Centrally manage the University IMIS and ensure continuity
d) Provide Helpdesks and end-user support to enable students and staff use ICT effectively
e) Extend access to learning through e-Learning support for distance learning
f) Support researchers by providing access to online resources and training on relevant courses
g) Integrate administrative and MIS systems to facilitate planning and decision making

h) Provide office productivity tools and facilities
i) Maintain efficient and effective ICT services at prescribed levels and standards
j) Ensure security of systems as per University policy
k) Protect systems against fraud and damage
l) Ensure clear lines of authority and delegated responsibility
m) Sustain ICT training and capacity building programmes to empower end-users
n) Performance benchmark bandwidth service levels with best practices internationally
o) Ensure e-waste disposal in accordance with socially acceptable environmental guidelines

Appendix A shows the structure of the ICT-Directorate

1.4   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 University's ICT Policy and therefore define it in detail**.

2   CONDITIONS OF USE OF COMPUTING AND NETWORK FACILITIES

a) It is the policy of the University that the ICT-Directorate computing and network facilities are **intended for use for teaching, learning, research, administration and management in support of the University's mission**. While recognizing the increasing importance of these facilities to the activities of staff and students, the University **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-Directorate from time to time.

c) It is the policy of the University that the ICT-Directorate computing and associated network facilities are not to be used for commercial purposes or non-University-related activities without written authorization from the University. In any dispute as to whether work carried out on the computing and networking facilities is internal work, the decision of the Vice-Chancellor or his delegate shall be final.

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

e) The University 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 University shall be under no liability in the event of any improper disclosure.

f) The University will endeavour to safeguard the possibility of loss of information within the University'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 University'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 university, or to any hardware or software failure which is beyond the end-user's means to avoid or control, then the ICT-Directorate will endeavour to help restore the information and will not surcharge the user for computer time spent in such restoration.

h) The use of the computing and network facilities is permitted by the University on the condition that it will not involve the infringement of any patent or the breach of any copyright and the end- user agrees to indemnify and keep indemnified the University and each and every member of ICT-Directorate staff against all actions, claims, and demands for infringement of patent and or breach of copyright which may be brought or made against the University or any member of the ICT-Directorate staff arising out of or in connection with the use of the computing and networking facilities.

i) End-users of the computing and network facilities recognize that when they cease to be formally associated with the University (e.g. no longer an employee, enrolled student or visitor to the University), they cease to be authorized users and access to the said facilities will be denied. In addition, their private information may be removed from University computing and network facilities without notice. Users must remove their private information and make arrangements for ICT-Directorate retention of any official University / School/ Division/ Departmental related information prior to leaving the University.

j) The University 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 against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

k) The University, 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 University disclaims responsibility and will not be responsible for loss or disclosure of user information or interference with user information resulting from ICT-Directorate efforts to maintain the privacy, security and integrity of the computing and networking facilities and information.

m) The University 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 University to take additional actions under this policy.

n) End-users of the computing and network facilities use the said facilities subject to applicable laws and University policies. The University disclaims any responsibility and/or warranties for information and materials residing on non-university computer systems or available over publicly accessible networks, except where such responsibility is formally expressed. Such information and materials do not necessarily reflect the attitudes, opinions, or values of the University, ICT-Directorate staff, or students.

o) The ICT-Directorate may disable or disconnect any person from using the computing and networking facilities (and may recommend additional penalties to the Senate and the Vice-Chancellor) if after appropriate investigation that person is found to be:-

 1. responsible for wilful physical damage to any of the computing and network facilities;
 2. in possession of confidential information obtained improperly;
 3. responsible for wilful destruction of information;
 4. responsible for deliberate interruption of normal services provided by the ICT-Directorate;
 5. responsible for the infringement of any patent or the breach of any copyright;
 6. gaining or attempting to gain unauthorized access to accounts and passwords;

7. gaining or attempting to gain access to restricted areas without the consent of the Director; and
8. responsible for inappropriate use of the facilities.

p) Cases requiring further disciplinary action will be dealt with in accordance with University disciplinary procedures

q) External work or use of the computing and networking facilities which would prevent University users from having their usual access to the facilities shall not be undertaken.

3 CODE OF PRACTICE IN THE USE OF COMPUTING AND NETWORK FACILITIES

3.1 Introduction

Standards for the use of the University'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 University community depends on a spirit of mutual respect and cooperation to resolve differences and resolve problems that arise from time to time. This code of practice is published in that spirit. The purpose of the ICT-Directorate is to specify user responsibilities and to promote the appropriate use of ICT for the protection of all members of the University community. The code of practice also applies to any other users authorised to access the University computing and network facilities

3.2 Appropriate and Reasonable Use

Appropriate and responsible use of the University computing and networking facilities is defined as use that is consistent with the teaching, learning, research, administrative and management objectives of the University 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.

3.3 Responsibilities

End-users of the University computing and networking facilities accept the following specific responsibilities:
1. 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 to control access to and use of administrative data.
2. Confidentiality:
   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 University;
   b) Not to represent others, unless authorized to do so explicitly by those users; and
   c) Not to divulge sensitive personal data to which they have access concerning staff or students without explicit authorization to do so.
3. To respect the rights of other users; for example, to comply with all University policies regarding sexual, racial, and other forms of harassment. The University is committed to being a racially, ethnically, and religiously heterogeneous community.

4. 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 or to share it with other users.

5. To respect the intended usage of resources; for example, to use only the account name and password, funds, transactions, data, and processes assigned by service providers, unit heads, or project directors for the purposes specified, and not to access or use other account names and passwords, funds, transactions, data, or processes unless explicitly authorized to do so by the appropriate authority.

6. 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.

7. 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-Directorate staff, academic staff, department and unit heads, project directors, or management staff.

8. To respect the financial structure of the computing and network facilities; for example, not to intentionally develop or use any unauthorized mechanisms to alter or avoid charges levied by the University for computing, network, and data processing services.

9. To adhere to all general University policies and procedures including, but not limited to, policies on proper use of information resources and computing and networking facilities; the acquisition, use, and disposal of University owned computer equipment including e-waste; use of telecommunications equipment; legal use of software; and legal use of administrative data among others.

10. To report any information concerning instances in which the University ICT Policy or any of ICT-Directorate standards and codes of practice has been or is being violated. In general, reports about violations should be directed initially to the administration of the school, institute, department , division or unit where the violation has occurred whereupon it will be passed on to the Custodian of the system. If it is not clear where to report the problem, it may be sent to the Information and Communications Technology Helpdesk which will redirect the incident to the appropriate person(s) for action or will handle it directly.

3.4 Information Ethics for Specific Activities

The following apply to specific activities.

3.4.1. Illegal activity
In general, it is considered inappropriate use to store and/or give access to information on the University computing and network facilities that could result in legal action against the University.

3.4.2. Objectionable material
The University'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
b) An article that describes or depicts, in a manner that likely to cause offence to a reasonable adult e.g.
   o The use of violence or coercion to compel any person to participate in, or submit to, sexual conduct;
   o Sexual conduct with or upon the body of a dead person;
   o The use of urine or excrement in association with degrading or dehumanizing conduct or sexual conduct;
   o Bestiality and all other sexual offences outlined in the Sexual Offences Act;
   o Acts of torture or the infliction of extreme violence or extreme cruelty.

3.4.3. Restricted Material

The University's computing and networking facilities must not be used to transmit or make available restricted material to a minor, restricted material being defined as an article that a reasonable adult, by reason of the nature of the article, or the nature or extent of references in the article, to matters of sex, drug abuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read or hear.

3.4.4. Restricted Software and Hardware

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 University 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. Authorization to possess and use Trojan horses, worms, viruses and password breakers for legitimate research or diagnostic purposes can be obtained from the Director, ICT-Directorate.

The unauthorized physical connection of monitoring devices to the computing and network facilities which could result in the violation of University 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 Director ICT.

3.4.5. 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. Because electronic information is volatile and easily reproduced or altered, respect for the work and personal expression of others is especially critical in computing and networking environments. Viewing, listening to or using another person's information without authorization is inappropriate use of the facilities. Standards of practice apply even when this information is left unprotected.
c) Most software that resides on the computing and network facilities is owned by the University or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. 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 University ; against the resale of data or programs, or the use of these for non-educational purposes or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization. University employees who develop new packages that include components subject to use, copying, or redistribution restrictions have the responsibility to make any such restrictions known to the users of those packages.
d) With a greater emphasis on computer based assignments, students need to be especially cognizant of the appropriate use of computing and networking facilities. In particular, academic dishonesty or plagiarism in a student assignment may be suspected if the assignment calling for independent work results in two or more solutions so similar that one can be converted to another by a mechanical transformation. Academic dishonesty in an assignment may also be suspected if a student who was to complete an assignment independently cannot explain both the intricacies of the solution and the techniques used to generate that solution. Suspected occurrences of academic dishonesty are referred to the Head of the student's academic department for action according to University's statutory rules and regulations.

3.4.6. Harassment

University policy prohibits sexual and discriminatory harassment. The University's computing and networking facilities are not to be used to libel, slander, or harass any other person. The following constitute examples of Computer Harassment:

a) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;

b) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

c) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease;

d) Intentionally using the computer to disrupt or damage the academic, teaching, learning, research, administrative, or related pursuits of another;

e) Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another; and

f) The display of offensive material in any publicly accessible area is likely to violate University harassment policy. There are materials available on the Internet and elsewhere that some members of the University community will find offensive. One example is sexually explicit graphics. The University cannot restrict the availability of such material, but it considers display of such material in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

3.4.7. Wasting Resources

a) It is considered inappropriate use of the computing and network facilities to deliberately perform any act which will impair the operation of any part of the computing and network facilities or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

b) The wilful wasting of computing and networking facilities resources is inappropriate use. Wastefulness includes but is not limited to passing chain letters, wilful generation of large volumes of unnecessary printed output or disk space, wilful creation of unnecessary multiple jobs or processes, or wilful creation of heavy network traffic. In particular, the practice of wilfully using the University's computing and network facilities for the establishment of frivolous and unnecessary chains of communication connections is an inappropriate waste of resources.

c) The sending of random mailings ('junk mail') is discouraged but generally permitted in so far as such activities do not violate the other guidelines set out in this document. It is poor etiquette at best, and harassment at worst, to deliberately send unwanted mail messages to strangers. Recipients who find such junk mail objectionable should contact the sender of the mail, and request to be removed from the mailing list. If the junk mail continues, the recipient should contact the appropriate local support person or the ICT Helpdesk.

3.4.8. Game Playing

Limited recreational game playing, that is not part of an authorized and assigned research or instructional activity, is not tolerated (except within the parameters of each department's rules). University's computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility must give up that position when others who need to use the facility for academic or research purposes are waiting.

3.4.9. Commercial Use

University computing and network facilities are provided by the University for the support of the university mission. It is inappropriate to use the computing and network facilities for:

a) Commercial gain or placing a third party in a position of commercial advantage;
b) Any non-university related activity, including non-university related communications ; and
c) Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the mission of the University or the service being provided.

This paragraph is not intended to restrict free speech or to restrict the University from setting up Information servers or other services specifically designated for the purpose of fostering an "electronic community" with the wider community the University serves. These designated Information servers should normally conform to the University's ICT Policy of which this Code of Practice is a part.

3.4.10.   Use for Personal Business

University'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 University, except in connection with scholarly pursuits (such as external examination, assessment or academic publishing activities). This and any other incidental use (such as electronic communications, downloads or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive.

3.5   Additional Guidelines at Local Sites

The University computing and network facilities are composed of many "sites." Each site may have local rules and regulations which govern the use of computing and network facilities at that site. Each site has operators, technicians, and/or supervisors who have been given the responsibility to supervise the use of that site. Each site has an administrator (Custodian) with overall policy responsibility for the site. Users are expected to cooperate with these individuals and comply with University and local site policies. Site policies may be more restrictive than the University policy. It is the intention that the University ICT Security Policy represents a minimum standard. Local administrators may impose more restrictive policies, which become their responsibility to administer.

3.6   Connection to the Campus-Wide Data Network

Most campus buildings are included in the Campus Network. To maintain the integrity of the University computing and network facilities, connections to the campus network are made only by specialized personnel under the direction of the ICT-Directorate staff. End -users are encouraged to connect appropriate equipment only at existing user-access points. All requests for additional network connections or for the relocation of a connection should be directed to the ICT- Directorate.

3.7   Use of Desktop Systems

End-users are responsible for the security and integrity of University 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. Users should avoid storing passwords or other information that can be used to gain access to other campus computing resources. Users should not store University passwords or any other confidential data or information on their laptop or home PC or associated floppy disks or CD's, or flash disks.

3.8   Use of External Services

Networks and telecommunications services and administrative systems and services to which the University maintains connections (e.g. Telkom, KDN, KENET) have established acceptable use standards. It is the user's responsibility to adhere to the standards of such networks. The University cannot and will not extend any protection to users should they violate the policies of an external network.

3.9   Printouts

Users are responsible for the security and privacy of printouts of University information.

4   APPROPRIATE USE OF ELECTRONIC MAIL

4.1   Statement

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

4.2   Scope

These Standards of Use cover all electronic mail systems used by members of the University community, from the University's network or connecting to the University's network or while acting in an official University capacity.

4.3   Appropriate Use and Responsibility of Users

Electronic mail can be both informal like a phone call and yet irrevocable like an official memorandum. Because of this, users should explicitly recognize their responsibility for the content, dissemination and management of the messages they send. This responsibility means ensuring that messages:
- a)   Do not contain information that is harmful to the University or members of the University community;
- b)   Are courteous and polite;
- c)   Are consistent with University policies;
- d)   Protect others' right to privacy and confidentiality;
- e)   Do not contain obscene, offensive or slanderous material;
- f)   Are not used for purposes that conflict with the University's interests;
- g)   Contain an accurate, appropriate and informative signature;
- h)   Do not unnecessarily or frivolously overload the email system (e.g. spamming and junk mail are not allowed); and
- i)   Are not for commercial purposes unless authorized by the University .

Users should cover periods of absence by adopting an appropriate functional account, forward, or vacation message strategy.
Electronic mail containing a formal approval, authorization, delegation or handing over of responsibility must be copied to paper and filed appropriately for purposes of evidence and accountability.

4.4   Data Backups

Although the ICT-Directorate will do everything possible to back up data stored on central server areas, it is the responsibility of the individual user to backup their own data from their computers, safely onto CD, diskette, or other storage media. It is the responsibility of the individual to store all information that is of value to the University on a recommended University supplied server.

4.5   Confidentiality and Security

a) Electronic mail is inherently NOT SECURE.
b) As University networks and computers are the property of the University, the University retains the right to allow authorized University officers to monitor and examine the information stored within.
c) It is recommended that personal confidential material not be stored on or sent through University equipment.
d) End-users must ensure the integrity of their password and abide by University guidelines on passwords (see section 5 below).
e) Sensitive confidential material should NOT be sent through the electronic mail system unless it is encrypted.
f) Confidential information should be redirected only where there is a need and with the permission of the originator, where possible.
g) 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.
h) Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users should verify authenticity with the ICT-Directorate.

4.6   User Indemnity

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

4.7   Limited Warranty

The University 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.

5   GUIDELINES ON PASSWORDS

5.1   Password Management
a) Passwords should be memorized - **never** written down.
b) Passwords belong to individuals and must **never** be shared with anyone else.
c) Passwords should be changed regularly at intervals of not more than three months, or immediately if compromised.

5.2   Password Administration
a) System Custodians should regularly run password cracking software against their password files to identify weak passwords.
b) New or changed passwords must be given in writing only to the identified user - never over the telephone or via email.

5.3   Password Construction
a) Users are advised to observe the following guidelines when choosing passwords:
b) A password should be at least 6 characters long.
c) Never make your password a name or something familiar, like your pet, your children, or partner. Favourite authors and foods are also guessable.
d) Never, under any circumstances, should your password be the same as your username or your real name.
e) Do not use words that can be associated with you
f) Do not have a password consisting of a word from a dictionary. Most basic cracking programs contain over 80000 words, and plenty of variations.

g) Try to have a password with a number or mixed case letters. Simple substitutions like a '1' for an 'i', and '0' for an 'O' are easily guessed. Add a '%' or '$' to the middle of the password.

6 STUDENT LABORATORY AND NETWORK CODE OF PRACTICE

6.1 Introduction

Your access to the Student Network is provided by the University for administrative, academic, research or study purposes only. The Student Network is a valuable but limited resource which must be shared with others. It is your obligation to use the facilities in an efficient, ethical, legal and responsible manner, in accordance with the University's "Code of Practice in the Use of Computing and Network Facilities", "Appropriate Use of Electronic Mail", and the code of conduct specified below. The "Student Laboratory and Network Code of Practice" is applicable to all student users, University staff and any other users authorised to access the student laboratories and network. Conduct that is considered grossly improper by the immediate system custodian may be grounds for termination of your access or be subject to other penalties which may apply.

6.2 Account Management

1. Your Student Network account is provided by the University in your name for your use only.
2. You must not share your account with family, friends or make your password available to any other person.
3. You should change your password at least every 3 months.
4. You may not use the account of any other person. If you inadvertently gain such access to any unauthorized information, you should advise Helpdesk staff immediately.
5. In certain circumstances you may share an account with others where shared duties apply. Such accounts will be specifically authorized by the Director ICT. In such cases all sharers are jointly responsible for the account but may not share with others outside the group.
6. You **must not** attempt to find the password of another user or access their account in an unauthorized username.

6.3 Identification

Computer Labs are provided for University students, staff and other authorised users. You must carry a valid University ID or other recognised form of identification at all times while using the labs. Security and Helpdesk staffs have the right to deny access to the Labs to anyone without proper identification.

6.4 Appropriate Electronic Behaviour

Users of the Internet are asked to comply with guidelines of network etiquette (netiquette). Netiquette is based on the use of good manners and common sense. Some are:
a) Always acknowledge electronic mail.
b) Limit your email to a single screen of text where possible.
c) Do not send large files as email attachments.
d) Do not use offensive language.
e) You must be polite to other users of the Internet.

6.5 Appropriate Use

Avoid wasting network resources:
File Transfer Protocol (FTP) should be used for academic and study purposes only. Download of music and video are not allowed unless express permission is obtained from the Director ICT.
The use of voice over IP (VOIP) wastes bandwidth and is discouraged. Limit use to 5-10 minute sessions only. Use of email is preferred. Do not attempt to talk to someone without obtaining their prior permission via email or similar.

6.6 Illegal Activities

a) Do not download or copy software without appropriate authority or license.
b) It is an offence to knowingly inject viruses into any system or engage in any other form of hacking.
c) 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.

6.7 Laboratory Etiquette

a) No food, drink or cigarettes are to be consumed in the laboratories.
b) Avoid excessive noise.
c) The number of workstations is limited. Please limit your sessions, especially if there are queues. Automatic termination of services may apply.
d) Please be courteous to staff and fellow users.
e) Game-playing is not desirable. It is forbidden when there are queues unless authorized in writing by your lecturer as part of your course.
f) You are required to comply with any instruction by a University staff member or security officer.

7 INTERNET CONDITIONS, STANDARDS, AND GUIDELINES

7.1 Introduction

The Internet introduces new opportunities and new risks. In response to the risks, this statement describes the University official policy regarding Internet security. It applies to all University employees, students, contractors, and temporary staff who use the Internet with University computing or networking resources, as well as those who consider themselves as being connected with the University.

7.2 Transmission of Information

a) Downloading

All software downloaded from non-University sources via the Internet must be screened with virus detection software prior to being invoked. Whenever the provider of the software is not trusted, down-loaded software should be tested on a stand-alone non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

b) Suspect Information

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of information is outdated or inaccurate.

c) Contacts

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

d) Information Security

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, University proprietary or private information must not be sent over the Internet unless it has first been encrypted by approved methods. Credit card numbers, log-in passwords, and other parameters that can be used to gain access to University systems, networks and services, must not be sent over the Internet in readable form.

7.3 Software Security

University computer software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-University party for any purposes other than University purposes, and these will expressly be authorized by School/Institute/Centre/ Deans or Director ICT.

Exchanges of software and/or data between the University 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. Regular business practices such as shipment of software in response to a customer purchase order need not involve such a specific agreement since the terms are implied.

The University strongly supports strict adherence to software vendors' license agreements. Adherence to these agreements **may involve** random audits by these vendors. When University computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

7.4   Personnel Security

a)   Privacy

Staff using University information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers should not send information over the Internet if they consider it to be private. Any doubts regarding the privacy of information should be resolved by contacting the ICT-Directorate.

b)   Right to Examine

At any time and without prior notice, University management reserves the right to examine e-mail, personal file directories, and other information stored on University computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of the University's information systems.

c)   Resource Usage

The University encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not University time. Likewise, games, news groups, and other non-University activities must be performed on personal, not University time. Use of University computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no University activity is pre-empted by personal use.

d)   Public Representations

Staff may indicate their affiliation with the University in bulletin board discussions and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address. In either case, whenever staff provide an affiliation, they must also clearly indicate the opinions expressed are their own, or not necessarily those of the University. All external representations on behalf of the University must first be cleared with the School Dean or Departmental Heads.

All staff must not publicly disclose internal University information via the Internet that may adversely affect the University's relations or public image.

7.5   Reporting Security Problems

Security problems or potential security breaches must be reported to the ICT-Directorate immediately. Such security problems are likely to occur when:

a)   Sensitive University information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.

b)   Unauthorized use of University information systems has taken place, or is suspected of taking place.

c)   Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.

d)   There is any unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages.

Security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not attempt to probe computer security mechanisms at University campuses or other Internet sites. If users probe security mechanisms, alarms will be triggered and University resources will needlessly be spent tracking the activity.

Unless prior written authority has been obtained from the Director ICT-Directorate, files containing hacking tools or other suspicious material may be taken as prima facie evidence of unauthorized hacking activity and may expose the user to disciplinary procedures.

7.6   Penalties
Violations of these computer security policies can lead to withdrawal and/or suspension of system and network privileges and/or disciplinary action.

8   STRATEGIC INFORMATION SYSTEM PLATFORMS
8.1   Definition of 'strategic'
A *strategic* system may be defined as a system that meets *several* of the following criteria:
- a)   Is critical to the mission of the University;
- b)   Affects large parts of the University;
- c)   Yields university-wide benefits; and
- d)   Is large

8.2   Management of strategic systems
The following policies apply in the management of strategic systems:
- a)   Strategic platforms will be managed and operated by the ICT-Directorate.
- b)   Strategic Applications will be managed by the designated custodian (such as Finance, Administration, Human Resource , Academic Department, and Research Division etc) of the application.

8.3   Physical security
The following standards of physical security of strategic platforms must be met:
- a)   Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.;
- b)   Air temperature and humidity must be controlled to within acceptable limits; and
- c)   Platforms must be electrically powered via UPS to provide the following:
    Minimum of 15 minutes' continuous operation in the event of a power blackout;
    Adequate protection from surges and sags; and
    Trigger an orderly system shutdown when deemed necessary.

8.4   Physical access
- a)   Premises will be staffed and controlled by designated ICT-Directorate staff.
- b)   External doors will remain locked, preferably with electronic locks and or grilled doors.
- c)   There will be security screens on all external windows.

8.5   User access
a)   New Users
New userids will be handled as follows:
- i.   Written application must be submitted on an official form;
- ii.   The application form must be signed by someone in authority (e.g. Dean, Director, HoD);
- iii.   The applicant must present suitable personal identification;
- iv.   The application form will be kept indefinitely by ICT-Directorate;
- v.   The new userid and password will be given orally to the applicant; unless special delivery has been authorized due to special circumstances (e.g. applicant is overseas);
- vi.   If the Operating System supports a password aging facility then it must be set to force password change on the first login; and
- vii.   The access level will be no higher than required as approved by the custodian.

b) Terminating Users

The userids of persons leaving the University or no longer requiring access will be disabled. All files will be referred to the system custodian for disposal.

8.6 Fire detection and control

a. There will be smoke and thermal detectors on the premises.
b. Under floor areas will have smoke and water detectors.

8.7 Data integrity

a. Security backups of all data will be made daily.
b. The backup regime must meet the following criteria:
   1. Enable recovery to at least the start of business on any weekday of a failure.
   2. Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.
c. There must be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.
d. There must be a validation of security backup media at least once every six months.

8.8 Password aging

If the Operating System provides the facility, automatic Password Aging will be enforced. The life of a password should be no more than 3 months.

8.9 Disaster recovery plan

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

8.10 Documentation

Procedures reflecting these policies must be documented by the ICT-Directorate.

9 SOFTWARE CHANGE CONTROL

9.1 Definition

Software Change Control covers the control of all aspects of strategic systems software including the operating system, ICT-Directorate associated packages (DBMS etc.) and utilities, third party and University in-house developed applications, together with any command procedures and documentation to support and run them.

9.2 General obligations

When changes are required to systems software, associated packages and utilities, applications software, command procedures, or documentation, it is essential that the changes are:

a) appropriately authorized and approved;
b) made in consultation with the Internal Audit section, where appropriate;
c) thoroughly tested;
d) sufficiently documented; and
e) Implemented at an appropriate time

Any change must only be transferred into the production environment when approved by the appropriate system Custodian.

Sound software security management requires that the procedures to manage the change control for applications and systems changes are clearly defined.

There must be a set of Software Change Control Procedures to assist the process indicating clearly the appropriate change-over process to be used i.e. pilot, phase, hot/cold in the case of existing systems.
All operational software relating to strategic systems should be placed under appropriate Configuration Management.

9.3   Change control responsibilities

Specific personnel will be given the responsibility for the implementation of changes by undertaking appropriate testing in the test environment, and, subject to the appropriate approvals, moving the changes to the production environment. All elements of the system will be subject to Software Change Control Procedures.
There should be a separation of responsibilities in the transfer of software from test into the production environment.

9.4   Change control environment

Where possible, three separate environments should be maintained for each strategic system:
1. development;
2. testing ; and
3. production.

Migration of software between environments should only be undertaken after obtaining the appropriate sign-offs as specified in the Software Change Control Procedures. New software and changes to existing software should be prepared in the *Development Environment* by appropriately authorized development or applications support staff. Applications should be specified, designed and coded according to University's systems development methodology.
Once assessed as satisfactory, the new or modified software should be transferred to the *Testing Environment* for systems and acceptance testing by an appropriate testing group, according to an agreed test procedure. Changes to software are not permitted in the testing environment.
Following successful completion of testing and approval by the appropriate systems custodian, the new or modified software should be transferred to the *Production Environment* for implementation under the control of ICT-Directorate staff. A contingency plan to enable the software to be restored to previous version in the event that the implementation is unsuccessful should be prepared where appropriate.

9.5   Documentation

a) **Change Control Procedures**
   Procedures reflecting these policies must be documented in the ICT-Directorate Software Change Control Procedures.
b) **Software Change Request**
   No software change is to be undertaken without an appropriately authorized Software Service Request. The Service Request is also the principal documentation to be completed for the software change management process.
c) **Technical, Operations and End User Documentation**
   Appropriate documentation in respect of each software change must be completed in sufficient detail and accepted before the change is implemented in the production environment.

10 COMMUNICATIONS NETWORK

10.1   Categorisation of Network access

Network access can be categorized into 3 major areas:

a) Campus Local Area Network ;
b) Intercampus Network (between future campuses); and
c) Wide Area Network (Internet).

The University has varying degrees of control decisions affecting security management of these areas:
a) Total control over the campus LAN links, given that university staff plan, install, manage, and maintain these systems.
b) Limited control over the Intercampus Network, which will be managed by a consortium of universities (KENET), Telkom, KDN and other providers.
c) No control over the Internet.

10.2 Campus Local Area Networks

a) Physical Security
The following standards of physical security in campus local area networks must be met:
   i. Premises housing network control equipment must be physically strong and free from unacceptable risk, flooding, vibration, dust, etc.
   ii. External building ducts must conform to university standards of service reticulation.
   iii. Internal building distribution of cables within ceiling, wall or floor cavities must be reticulated within protective conduits.
   iv. Air temperature and humidity must be controlled to within equipment defined limits.
   v. Network electronics must be powered via Un-interruptible Power Supplies to provide the following:
      1. Minimum of 15 minutes' operation in the event of a power blackout.
      2. Adequate protection from surges and sags.

b) Physical Access
   1. Access to areas housing network electronics will be controlled by designated ICT-Directorate staff.
   2. Doors to areas housing network electronics will be locked with a unique key, the distribution of which will be determined by Director ICT.

c) Data Integrity

i) Eavesdrop Protection
By utilizing eavesdrop protection at the network hardware level, full network flexibility on campus is retained at the user end, with an unbreakable system of eavesdrop protection.
The University Campus Local Area Networks should all be protected by a hardware level of eavesdrop protection.

ii) Intrusion Protection
Within the boundaries of the LAN, intrusion protection is required to prevent:
   1. Non-university staff or students from indiscriminately connecting laptop computers to any access point of the campus network
   2. Unauthorized access of staff and students to the Universities strategic systems.
   3. Only those computers belonging to staff and students will be allowed to function when connected to the University network. Visiting personnel wishing to access the network must have authorization from a university staff member, who must apply to ICT-Directorate for temporary access rights.
   4. No undergraduate student should be allowed Telnet or FTP access to strategic computing systems.

10.3   Inter-campus Network

The planned inter-campus network could be supported via a combination of leased Fibre Optic backbone cable and leased or private wireless system operated and managed by the University ICT-Directorate will be explored. The ICT-Directorate will ensure that:

a) Appropriate CCK licensing is sought for all wireless frequencies being used for data transmission between future campuses.
b) Wireless equipment uses "focused" transmission techniques between transmitting and receiving dishes and that "non-focused" transmission is only used for non-secure data (e.g. broadcasting teaching material into the public arena).
c) Wireless repeater sites are secure - refer to Campus LAN physical and access security above.

10.4   Wide Area Networks

Protection from illegal entry from public Wide Area Networks is usually provided by network firewalls. However, with the diverse nature of the University's business and the public nature of the services that it delivers, firewall solutions are not sufficient. Many of the University's prospective clients are external to the campus and use the public networks to access the university teaching, research and library material. Also, academic staff can be highly mobile, requiring access to the University's network from various external locations, even from overseas.

Because of the nature of Wide Area Networks (WAN) there are only limited security measures that can be taken. Security Policy for Strategic Systems must rely heavily on software applications and general computer controls. The risks of transmitting information over the WAN must be considered when:

a)   Determining the nature of information to be sent over the WAN
b)   Granting approval for new applications which involve the transmission of information over the WAN.

11 DEPARTMENTAL COMPUTER SYSTEMS

11.1   Introduction

'Departmental' systems are non-strategic servers (i.e. not desktops) that are the responsibility of Divisions, Schools, Departments, Offices, or Centres (Learning centres). Responsibility for the management and operation (i.e. custodianship) of departmental systems resides with the department that owns the system.

The day-to-day security responsibilities lie with managers of departmental systems who must:

a) Be thoroughly familiar with the University's ICT Policy in its entirety;
b) Ensure compliance to this policy by all of Department's users.; and
c) Report any serious breaches of security to ICT-Directorate.

11.2   Physical Security

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

a) Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.;
b) There must not be an inordinate amount of combustible material (e.g. paper) stored in the same room as the computer system; and
c) Air temperature and humidity must be controlled to within acceptable limits.

Computing equipment should be electrically powered via UPS to provide the following:

a) Minimum of 15 minutes' operation in the event of a power blackout;
b) Adequate protection from surges; and

c) Trigger an orderly system shutdown when deemed necessary.

11.3   Physical Access

There must be procedures in place to assure that only authorized staff enters the premises.

11.4   User Access

New userid's should 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. Dean, HoD);
- c) The applicant must present suitable personal identification;
- d) The userid and password must be given orally to the applicant; unless special delivery has been authorized due to special circumstances (e.g. applicant is overseas); and
- e) If the Operating System supports a password aging facility then it should be set to force password change on the first login.

11.5   Fire Detection and Control

There should be smoke and thermal detectors on the premises.

11.6   Business Continuity

There should be a Business Continuity evaluation along the following lines:
1. A determination the maximum time of not having the service(s) provided by the system that can be tolerated. This will be determined by the ICT-Directorate having carried out an evaluation of the relevant systems.
2. An identification of all of the threats to the system such as:
    a. Hardware Failure;
    b. Electrical Power Failure; and
    c. Fire.
3. Formulation of Contingency Plans for restoring services within the acceptable time. The ICT-Directorate will give advice on risk management and contingency planning.

11.7   Data Integrity

a) Security backups of all data will be made at least once per working day. However, certain security backups will be made at the end of every data batch whenever specific requests are placed by a department, or whenever it is considered absolutely necessary by the relevant department at the ICT-Directorate.
b) The backup regime should 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.
c) There should be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.
d) There should be an audit of security backup media at least once every six months.

11.8   Password Aging

If the Operating System provides the facility, automatic Password Aging should be enforced. The life of a password should be not more than 3 months.

11.9   Documentation

Procedures reflecting these policies be documented in the site Operations instructions.

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 University's ICT Policy.

12.3   Hardware Security

The following guidelines apply:
   a) Lock offices. Office keys should be registered and monitored to ensure they are returned when the owner leaves the University;
   b) Secure Desktops in public areas. Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case;
   c) Secure hard disks. External hard disks should be secured against access, tampering, or removal;
   d) Mark departmental computers clearly with the access control numbers of the University;
   e) Locate computers away from environmental hazards;
   f) Store critical data backup media in fireproof vaults or in another building; and
   g) Register all University computers.

12.4   Access Security

Utilize password facilities to ensure that only authorized users can access the system. Where the desktop is located in an open space or is otherwise difficult to physically secure then consideration should be given to enhanced password protection mechanisms and procedures.
Password guidelines:
   a) Length 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 should not be maiden names, or names of children, spouses, or pets.) ;
   d) Do not write passwords down anywhere;
   e) Change passwords periodically; and
   f) 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; and
c) Fix software problems immediately.

12.6   Confidential Information

a) Encrypt sensitive and confidential information where appropriate;
b) Monitor printers used to produce sensitive and confidential information; and
c) Overwrite sensitive files on fixed disks, floppy disks, or cartridges.

12.7   Software

Software is protected by international Copyright law. Anyone who uses software should understand and comply with the license requirements of the software vendor. The University may be subject to random license audits by software vendors.

12.8   Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.
To decrease the risk of viruses and limit their spread:
a) Check all software before installing it;
b) Use software tools to detect and remove viruses; and
c) Isolate immediately any contaminated system.

12.9   Computer Networks

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.
While the ICT-Directorate 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) 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 University's networks;
c) Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers;
d) Always **back up** your important files;
e) Use (where appropriate) encrypting/decrypting and authentication services to send confidential information over the University network; and
f) Never store University passwords or any other confidential data or information on your laptop or home PC or associated floppy disks or CD's. All such information should be secured after any dialup connection to the University network.

13 COMMUNICATIONS NETWORK MANAGEMENT

13.1 Introduction

High quality communications are essential to support the mission of the University. The University's Communications Network is comprised of communications infrastructure, equipment, and standards associated with the transport of data, telephony, radio and ancillary communications services, throughout the University.

The ICT-Directorate will be responsible for the overall management of the Communications Network, managing and administering appropriate standards to ensure consistency and quality of communications services. Strategic planning, investigation and adaptation of new technologies, capacity planning, and maintenance of appropriate databases and records are also the responsibility of the ICT-Directorate.

13.2 Service levels

13.2.1 Accessibility
a) All staff and students where appropriate, will be provided with access to voice and data services.
b) All staff and students located off-campus will be provided with dial-in access to data services.
c) Associated organizations, located at the University's campuses, may be allowed access to the Communications Network.
d) Switchboard, Helpdesk and telecommunication support services will be provided by ICT-Directorate.

13.2.2 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.

Equipment downtime will be minimized through the use of redundant, self-healing communications designs. Where redundant designs are not an option, downtime will be minimized through the use of automatic fault alert systems, on-site spares and after-hours monitoring. Every effort will be made to ensure that externally provided communication services are also able to provide maximum up time.

Efficient fault reporting mechanisms and fault escalation procedures will continue to be implemented, to provide a means by which all faults can be easily reported and promptly resolved.

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

13.2.4 Capacity and Growth
The ICT-Directorate maintains adequate expansion capacity in infrastructure and equipment to ensure minimal delay in the provision of telephone and network services, supported by a fundamental strategy of providing:
a) Separate physical locations for key redundant equipment;
b) Separate redundant routes to all major buildings;
c) Automatic re-routing of key services to an alternate path/provider in the event of primary path/provider failure;
d) Short-term emergency power to critical distribution points;
e) Industry standard, integrated cabling and infrastructure in all buildings;
f) Progressive migration towards an integrated voice and data system; and
g) Increase LAN coverage through wireless access points.

13.3   Proprietary Internet Service Provision

The University will actively solicit educational discounts from Internet Service Providers (ISPs). Such discounts will be negotiated *a priori* with such ISPs as part of their documented corporate policy. The University will pay careful attention to the Terms and Conditions associated with such discounts.

14   ICT EQUIPMENT DISPOSAL

14.1   Purpose

This part of the policy is to establish and define standards, procedures, and restrictions for the disposal of non-leased ICT equipment in a legal, environmentally friendly and cost-effective manner. The University's 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 University's upgrade guidelines. Therefore, all disposal procedures for retired ICT equipment must adhere to University-approved methods and also the government disposal and boarding standards.

14.2   Scope

This applies to the proper disposal of all non-leased University equipment including PCs workstations, laptops, printers, mobile phones, PDA's and other hand-held devices, servers, switches, routers, and so on. University-owned surplus equipment, obsolete equipment, and any equipment beyond reasonable repair or reuse are covered by this policy. Where applicable, it is desirable to achieve some residual value of the equipment in question through reselling, auctioning, donation, or reassignment to a less-critical function.
It is important to note that most equipment will have little or no value once beyond the primary and secondary deployment timeframe. It is important to be realistic as in most cases, resale value will be small or zero.

14.3   Definitions

"**Non-leased**" refers to any and all ICT equipment that is the sole property of the University ; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company. This includes equipment purchased through a University Research grant.

"**Disposal**" refers to the reselling, recycling, donating, or discarding of ICT equipment through responsible, ethical, and environmentally sound means.

"**Surplus**" refers to hardware that has been replaced by upgraded equipment or is surplus to existing requirements.

"**Beyond reasonable repair**" refers to any and all equipment whose condition requires repair or refurbishment that is likely cost equal to or more than total replacement.

"**Primary Deployment**" refers to the time period for which new equipment should be used.

"**Secondary Deployment**" refers to a period of up to two years after the completion of the primary deployment of the ICT equipment.

14.4 **Guidelines**

Disposal of surplus ICT equipment (that are assets) will follow existing policy associated with the disposal of the equipment and all paperwork must be completed by the requestor.

14.5 **Practices**

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

Acceptable methods for the disposal of ICT equipment are as follows:
   a) Used as a trade-in against cost or negotiated discount rate of replacement or associated item. This option is only available for some manufacturers;
   b) Donated to schools, charities and other non-profit organizations; and
   c) Discarded as per socially acceptable environmental guidelines in liaison with a credible third party.

It is the responsibility of any employee of the University with the appropriate authority to ensure that ICT equipment is disposed of according to one or more of the methods prescribed above. It is imperative that any disposals performed by the University are done appropriately, responsibly, and ethically, and with University resource planning in mind. The following rules must therefore be observed:

Trade-Ins: Where applicable, in cases where a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old equipment against the cost of the replacement. The Director ICT will assume this responsibility.

Income Derived from Disposal: Whenever possible, it is desirable to achieve some residual value from retired or surplus ICT equipment, although any returns are expected to be small. Any and all receipts from the sale of the equipment must be kept and remitted to the department that owned the equipment. Income derived from sales to public must be fully receipted and paid to the University cashier.

Cannibalization of Equipment beyond Reasonable Repair: The Director ICT is responsible for verifying and classifying any equipment beyond reasonable repair. Equipment identified as much should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the organization. ICT-Directorate will inventorize and stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means will be disposed of according to socially acceptable environmental guidelines.

Decommissioning of Equipment: All hardware slated for disposal, by any means, must be fully wiped clean of all University data and software. ICT-Directorate will assume responsibility for decommissioning this equipment by deleting all files, University-licensed programs, and applications using a pre-approved disk-sanitizer. This sanitizer must completely overwrite (2x) each and every disk sector of the machine with zero-filled blocks.

Harmful Substances: ICT equipment contains hazardous materials such as lead, mercury, bromine, cadmium, etc. ICT-Directorate is responsible for selecting and approving external agents for the disposal of redundant equipment according to socially acceptable environmental guidelines.

Donations: Retired ICT equipment may be donated to a University-approved school, charity, or other non-profit organizations. All donations must be authorized by the Vice-Chancellor.

14.6   Disposal of Ink Cartridges and related waste

Used ink cartridges and other waste emanating from computer consumables will be disposed of according to University environmental guidelines. The ICT-Directorate will also liaise with printer manufacturers, re-sellers or any other third parties who will accept used cartridges for recycling or disposal in environmentally appropriate ways.

15   COMPUTERS AND RELATED ACCESSORIES PROCUREMENT

15.1   Governance

15.1.1   ICT Board

This statutory committee will be chaired by the Deputy Vice-Chancellor. The powers of the Board are to:

a) Consider and recommend ICT policy, strategies and plans in line with University priorities;
b) Consider and recommend ICT budget and the allocation of ICT resources among users;
c) Consider and consolidate ICT requirements for various University functions, staff and students;
d) Facilitate (and monitor) implementation of large ICT projects;
e) Consider and recommend quality of service measures to enhance service delivery to various cadres of end users
f) Scrutinize any hardware and software license agreements with vendors and service level agreements with Internet Service Providers and advise Management Board and Senate accordingly; and
g) Address any other ICT strategic and policy matters as may be referred to it by the Management Board and Senate.

15.1.2   School, Institute, Centre, Department ICT Committees

Schools/Centres will constitute ICT committees. The School ICT committee will help the School prioritise replacements and identify needs for new equipment and training.

15.2   Purchase of computers and related equipment

The ICT-Directorate will approve all specifications for servers, workstations, PCs and related equipment purchased by the University's Procurement Office in accordance with the Public Procurement and Disposal Act (2005). The ICT-Directorate, as stated elsewhere in this policy, will manage and control all PCs and related equipment on a University-wide basis. The ICT-Directorate will evaluate and consolidate the needs of each department and make recommendations on specifications for computers, servers and other accessories. All purchases will be carried out following the University's statutory procurement procedures.

When equipment is delivered to the University, the ICT Director will verify that it conforms to the university's specifications. The Purchasing Office may not purchase any servers, workstations, PCs or related automation equipment outside the University policy and without approval of Director ICT.

15.3   Purchase or Lease

It is the policy of the university to purchase rather than lease computers or lease high-end servers. However, on a need basis, especially for short term use, a lease arrangement can be agreed on with the approval of the Vice-Chancellor's office.

15.4   Laptops and Notebooks

Laptops and notebooks purchase is limited and staff members are encouraged to buy own laptops. Staff will get support to buy own laptops on a check-off basis, under a scheme to be initiated by the Vice-Chancellor. The University will participate in projects sponsored by the private or public sector to enhance student access to laptops and PCs. The terms and conditions for participating in such projects will be vetted by the ICT-Directorate on behalf of the University.

15.5 Computer Warranty

All PCs carry a warranty as a standard. The warranty will include on-site repair and parts replacement. The minimum warranty is at least one year.

15.6 Computer Brand and Quality

The university will not purchase non-branded computers.

15.7 Equipment donations

Donations of computers and other ICT equipment made to the university will be accepted if the equipment meets the immediate needs of the university as stated in the ICT Policy and Strategy. The ICT-Directorate will verify the specifications of the donated equipment, in consultation with the department or unit where the equipment will be deployed. The Vice-Chancellor will retain the authority to accept or reject an equipment donation.

15.8 Educational discounts

The University will actively solicit educational discounts from manufacturers of branded hardware and or software. Such discounts will be negotiated *a priori* with such manufacturers or software houses as part of their documented corporate policy. The University will pay careful attention to the Terms and Conditions associated with such discounts.

16 ICT EQUIPMENT LIFECYCLE

16.1 Introduction

This part of this policy is to establish and define a lifecycle for all ICT equipment. This is intended to provide a balance between optimum use and on-going maintenance costs to enable staff to use the latest software with ease.

16.2 Scope

This applies to all University owned and leased ICT equipment including PCs , workstations, laptops, printers, mobile phones, PDA's and other hand-held devices, servers, switches, routers, etc.

16.3   Definitions

"**Primary Deployment**" refers to the time period during which new equipment should be used.
"**Secondary Deployment**" refers to a period of up to two years after the completion of the primary deployment of the ICT equipment.

16.4   Guidelines

The University will maintain a multiple year lifecycle for all University owned and leased ICT equipment to ensure that it is replaced on a regular basis. ICT equipment becomes more expensive to service and support as it grows older. All ICT equipment purchased will be subject to a defined deployment life-cycle. Two types of deployment lifecycles exist that relate to the use of the equipment, either Primary or Secondary deployment. Primary Deployment of ICT equipment is that which has a "life" of up to the time-frames as shown in the table below, after which time it is replaced or deemed suitable for secondary deployment. Such equipment is utilised in high use and high availability areas, and must be covered (where possible) by full on-site warranty and associated support levels. In the case of critical equipment, it may also be effective to retain on-site spares (with a "return to base" or consignment arrangement) that can be replaced at short notice and returned to the manufacturer for repair. The time-frames normally reflect manufacturers normal and extended warranty periods for new ICT equipment.

16.5   Primary Deployment Time Frames (recommended)

Equipment Type	Deployment
PC Workstations	3 years
PC Laptops	3 years
Printers	4 years
Mobile Phones, PDA's & other	2 years
Servers	5 years
Switches and Routers	5 years
All other ICT equipment	3 years

Secondary Deployment occurs where equipment is reassigned to a less-critical role. It is the goal of the University to, whenever possible; reassign ICT equipment in order to achieve full return on investment (ROI) from the equipment and to minimize expenditure on new hardware when feasible reassignment of retired equipment deemed suitable for secondary deployment to another business function will do instead. Secondary deployment can occur for a period up to a maximum of two years, per the table below.

16.6   Secondary Deployment Time Frames (recommended)

Equipment Type	Deployment
PC Workstations	2 years
PC Laptops	1 year

Printers	2 years
Mobile Phones, PDA's & other	1 year
Servers	2 years
Switches & Routers	2 years
All other IT equipment	1 year

After this time, the equipment may be considered "obsolete "and plans made for replacement. Where such obsolete equipment is still running and its in-house maintenance costs are reasonable and spares are readily available in the market, the ICT-Directorate will use its discretion before designating it as obsolete.   Once, however, equipment is formally classified as being "obsolete", they must be disposed of according to the ICT Equipment Disposal policy.

16.7   Deployment areas
Deployment of ICT equipment is based on the following:

Primary Deployment	All Staff, students for normal day-to-day use in computer laboratories and offices. This includes part-time students, post-graduate students and researchers.
Secondary Deployment	Data logging and collection, instrumentation, computer controlled devices and for general purposes such as shared casual usage. Testing, experimentation, spare parts, testing and temporary use where the technical specifications are compatible.

17 ICT NETWORK CABLING INFRASTRUCTURE STANDARD
17.1   Introduction

This standard provides the minimum installation and operational requirements for University cabling systems. This standard applies to all ICT cabling (voice, data, audio and visual cabling), in horizontal cabling, backbone cabling, and inter-building cabling. The standard is to be applied to all copper and fibre optical cabling within all University campuses and buildings, regardless of their intended use.

17.2   Scope

The principles of the standard must be applied when conducting cabling projects for:
   a)   The construction of new buildings;
   b)   Fit outs of existing buildings;
   c)   Upgrades to existing cabling infrastructure; and
   d)   Implementation of cabling infrastructure to interconnect new or existing buildings.

18 PRIVACY
18.1   Introduction

This part of the policy covers information in any form, and includes, but is not limited to, information held on:
   a)   paper ;
   b)   audio or videotape;
   c)   microfilm or microfiche;

d) computer chip-based memory;

e) any magnetic or optical medium, such as computer disks.

18.2   Collecting Personal Information

The privacy of your personal information is important to the University .The University will collect personal information only when it is necessary for the University's functions or activities, and will collect sensitive information only when you have consented, or if the law requires us to collect the information.

When your information is collected, the University will take reasonable steps to advise you of the collection, and that you have a right to know, generally, who is collecting the information, for what purposes, and what sort of personal information is held. You will grant your consent by way of a signed Consent Form.

Where it is reasonable and practicable to do so, your personal information will only be collected directly from you. If it is necessary to collect personal information from a third party, reasonable steps will be taken to ensure that you are informed.

Reasonable steps will be taken to ensure that personal information holdings are relevant, accurate, up to date, complete and not excessive.

If you are able to establish that the information is not accurate, complete and up-to-date, we will take reasonable steps to correct the information. Should we disagree with you, we will take reasonable steps to associate the information with a statement from you claiming that the information is not accurate, complete or up-to-date.

 The University will not use or disclose information, other than for the purposes for which it was collected, unless you have consented, or you would reasonably expect the information to be used for the secondary purpose.

The University will not disclose information outside of the University or ICT-Directorate authorised contractors (even to parents, employers or the police) without your consent, except where:

a) the University is required by legislation, court order or other legally enforceable instrument and the request is in an appropriate written form; or

b) disclosure is reasonably believed to be necessary to prevent or lessen a serious and imminent threat to the life or health of any person; or

c) there is a request from:

   i. another university to obtain information on the academic record and performance of a student, including whether the student was expelled or suspended for disciplinary reasons

   ii. a third party to confirm whether a person is a graduate from the University with a particular qualification (noting that this information is publicly available through University publications);

The University will take reasonable steps to confirm the legitimacy of the request and requesting organization.

The University will take reasonable steps to protect the personal information we hold from misuse and loss, and from unauthorised access, modification or disclosure.

Personal information will be retained for only as long as it is needed and then disposed of lawfully and securely.

18.3   Personal Information

Personal information is information or an opinion, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Examples of personal information are your:

a) address – postal or residential;

b) telephone or fax numbers;

c) photograph ;

d) date of birth;

e) gender;

f)   academic results or qualification;
g)   disciplinary record ;
h)   debt to the University; and
i)   banking details and account number.

18.4   Sensitive Information

Sensitive information is information or an opinion about your:
a)   racial or ethnic origin;
b)   political opinions;
c)   membership of a political organization;
d)   religious beliefs or affiliations;
e)   philosophical beliefs;
f)   membership of a professional or trade association;
g)   membership of a trade union;
h)   sexual preferences or practices;
i)   criminal record ; and
j)   health.

Violation of this privacy policy may result in disciplinary action under the 'Conditions of Use of Computing and Networking facilities'

19 ICT FOR TEACHING, LEARNING AND RESEARCH

19.1   Teaching and Learning

ICTs will be used to support teaching and learning at the University . Emphasis will be on e-learning and other blended learning approaches.
In this policy document, teaching and learning includes instructional design and delivery, assessment and anti-plagiarism. ICT is core to the realisation of innovative teaching and learning that is supported by these three aspects.
Various infrastructures will be put in place to support networked learning and other e-learning approaches. All lecture halls will be fitted with state-of-the-art facilities that will enable the implementation of e-learning and other blended learning approaches. As a minimum standard, all lecture halls will be fitted with infrastructure for multi-media teaching and learning.

19.2   Anti- Plagiarism and Quality Assurance

The University recognizes that the Internet is a powerful 21st century research tool that cannot be ignored in a university environment. Whereas access to the Internet for academic and research work is encouraged, the University also realizes that it is possible for some students to copy other peoples work from the internet and present it as their own.
Most of the students work, assignments or thesis is presented in paper format. It is a difficult task for lecturers to countercheck for plagiarism from paper based submissions. This then leaves a doorway for dishonesty and by extension, poor quality and undeserving graduates.
The University recognizes that use of electronic means to track plagiarism is an important element of e-learning.
It is therefore University policy that:
a)   Student assignment, theses or project work will be presented in soft copy on CDs and, also paper copy.
b)   That all submitted work will be tested for plagiarism using University authorized software
c)   That all lecturers continue to acquaint themselves with usage of the anti-plagiarism software and will be required to ensure that no final marks are awarded before plagiarism is tested.

19.3   Assessment

With the increased enrolments in university classes in all public universities, one major challenge is to maintain robust systems of conducting Continuous Assessment Test (CATs) as per university assessment policy and have the transcripts ready on time. It has become an expensive and time consuming exercise and sometimes some universities are unable to provide results in time or provide adequate number of CATs.

The University recognizes assessment as an important part of quality assurance and places a great deal of importance on this. To this end, electronic means of assessment is considered an important part of e-learning that will have an impact on uniformity of assessment, and help reduce costs associated with examinations. This assessment will be for both on-campus and off-campus students where possible.

It is therefore University policy that:
   a) Where possible, electronic continuous assessment will be designed and delivered to students on a regular basis
   b) All exams will be regulated and approved by relevant University organs
   c) The assessment system will become a mission critical system that will be secured and provided with redundancy to ensure that exams proceed in case of any system failure.
   d) The University will provide the infrastructure and software needed to support provision of the assessments.

19.4   Virtual Learning Environment (VLE)

The Virtual Learning Environment offers the students a holistic environment for learning while providing instructors, lecturers and professors with effective teaching and research environment. The University's approach would be to use a platform that provides students with an open learning facility that can be used from anywhere and anytime in the world.

The University identifies Learning Management System (LMS) as a crucial component of VLE. It is University policy that the LMS should have the following key features:
   a) User friendly;
   b) Open architecture features that support third party add-ons;
   c) Scalability and modularity that allows for growth of content;
   d) Support multi-user access from many students and other users;
   e) SCORM compliant;
   f) Good security features that allow for different levels of security;
   g) Support assessment;
   h) Easy to update by lecturers; and
   i) Assessment features for testing on line with effective results summary and feedback.

It is University policy that where possible and desirable, open source e-learning systems will be used to reduce cost and also allow for customization.

19.5   Video Conferencing

The Internet provides an excellent platform for wide reach and is easily accessible anywhere in the world so long as appropriate infrastructures are put in place. One of the key applications of the Internet is the World Wide Web. It is possible to have highly interactive simulated graphics and video conferencing that can enhance a students learning experience.

However, the University believes that students still need a touch of the face to face lectures from the lecturers and professors. As result the University seeks to exploit video conferencing capabilities of the web, ISDN, VSAT and other technologies so that lectures can be taken not only from out of campus distant learning centres but also on campus by lecturers at distant locations any where in the world.

It is therefore university policy that video conferencing be seen as part of the e-learning infrastructure. Video conferencing should:

a) Be a multi-point system, capable of simultaneously connecting more than two sites through the use of a multi-point control unit.
b) Have dial out capability allowing the use of multiple telephone lines to connect two or more sites in the same conference.
c) Be compliant with International Telecommunication Union (ITU) standards such as H.323 and H.320 as well as data standards.

19.6   e-Learning Centre

To coordinate and manage use of ICT in teaching and learning, the University intends to establish a Center for e-Learning in accordance with Statute XXXIX. The University will work with partners to support the Centre for e-Learning to provide university curriculum in designated fields to learners outside the established campuses.
It is therefore the University's policy that the Learning Centres will be facilitated with:
a) Appropriate tools to facilitate student participatory learning from a distance
b) Communication channels, such as email to enable students communicate among themselves and with their lecturers
c) Access to the Internet to ensure that students participate in research
d) Learning Centre supervisors to ensure that the student needs are adequately addressed and university interest are taken care of.
e) Support technicians to ensure that all technical problems are addressed
f) Trainers and technicians to provide basic training on ICTs to new students on use of facility(s).
The Director, Centre for e-Learning and other staff at the e-Learning Centre will perform their roles as defined in the University Open, Distance and e-Learning (ODEL) Policy.

20 SKILLS DEVELOPMENT

In order to facilitate the implementation of the different ICT services and systems, considerable knowledge and skills must be developed among all levels of potential users. This will enable them to use ICT services and systems effectively and independently, and also to be aware of the shared responsibilities.

The University intends to develop the capacity of all users in the University to operate comfortably and efficiently in an environment where most pedagogic, administrative and managerial processes are ICT based. This will enable users to fully utilize the services and systems, and also to develop, implement and maintain them effectively. They will be able to exploit the full potential of the technologies.

The University will require that all students, academic staff, administrative and support staff are trained on a continuing basis to equip them with the requisite skills to exploit the functional potential of ICT. It is expected that as a minimum standard, all staff and students will be able to use standard application packages (word processors, spreadsheets and databases), e-mail and the Internet. Routine administrative tasks like calling meetings, notices and distribution of various documents will be done online. It is also expected that students and staff will interact more using e-mail and online discussion forum.

APPENDIX A

Structure of the ICT-Directorate