TAKORADI TECHNICAL UNIVERSITY

ICT SERVICES AND SYSTEMS; MANAGEMENT, CONTROL, MAINTENANCE AND USER POLICY

Takoradi Technical University
P. O. Box 256,
Takoradi - Ghana,
West Africa.

Website: www.ttu.edu.gh
Email: info@ttu.edu.gh
Tel: +233 (0) 312 025 162
Fax: +233 (0) 312 025 256

TABLE OF CONTENTS

Preamble	01
Drivers of the Policy	01
ICT Management	02
Data Communications Infrastructure	07
Management Infrastructure System	11
Software	13
Security	15
Management of Institutional Data	16
Information Technology Standards	20
University Computer Equipment	21
ICT Procurement	23
Resource Distribution	23
General Responsibilities of ICTSU	24
Repair of Computer Equipment	26
Asset Disposal	26
Data Backup	30
Employee Departure Chechout Checklist	33

Internet/ Intranet Usage 35

Computer Security 36

Official Electronic Mail Usage 38

Virus Protection 41

Password Management 45

The Appropriate Use of other ICT Resources 49

End User Skills Development 51

Enforcement and Penalties for Violations 54

Computer Disaster Recovery 55

1.0 PREAMBLE

Nations worldwide have recognised the developmental opportunities of Information and Communications Technology (ICT). ICT is playing an increasing role in many societies worldwide. From the local to the global level, ICTs have permeated all areas that pertain to socio-economic development, and are enabling the development of new skills, competitiveness and growth, particularly in developing nations. It is against this backdrop that the Government of Ghana launched "The Ghana ICT for Accelerated Development (ICT4AD) Policy". The main objective of that policy is to engineer an ICT-led socio-economic development process with potential to transform Ghana into a middle income, information-rich, knowledge-based and technology driven economy and society.

In line with the objective of Ghana's ICT Policy, the Takoradi University, herein after called "the Institution" which is mandated to train middle and top level human resource for national development, deems it fit to have an ICT Policy in place. This Policy shall serve as a guide to all Staff, Students and other stake holders of Takoradi University with respect to how the computers, networks facilities (Internet, intranet, and extranet) and all other ICT accessories would be acquired, managed and utilised. The Institution by this policy states that all its ICT facilities are to be used for Research, Educational and administrative duties that support achievements of the institution's objectives only.

2.0 DRIVERS OF THE POLICY

2.1 Vision

To utilise ICT to facilitate teaching, learning and management of data of the University to ensure value returns on investment in Information Communication system resources in order to position

the University as a centre for academic and technological excellence.

2.2 Mission

To establish a World Class ICT system services in partnership with stakeholders for sustainable institutional development.

2.3 Scope

This policy applies to any person accessing/developing/implementing and/or using ICT-based information and ICT resources owned, managed, supported or operated by, or on behalf of, the Institution.

The Policy is applicable to:

1. All ICT systems and electronic records owned by or licensed to the Institution.

2. All individuals who are granted access to ICT resources and facilities owned and operated by the Institution, including but not necessarily limited to, staff, students, researchers, and visiting scholars.

3.0 ICT MANAGEMENT

ICT management involves the adoption of complimentary strategies in three key areas:

i. Budgeting and finance

ii. Human resource

iii. Policy and best practice

To derive more value from organizational ICT investment, ICT management requires flexibility, constant learning and apprecia-

tion of the specific implementation of ICT.

The Institution has decided on the following general policies for the development and sustainability of appropriate Information Resources Management (IRM) capabilities. The general policy includes short-term IRM policies, long-term IRM policies and ownership policies.

It is the University Policy to ensure sustainable management of the University's ICT policy and resources through the creation of appropriate policy, advisory, management and operational organs that shall cater for the broad interests of all users. It is the University Policy to provide for the growth and financial sustainability of its ICT resources through appropriate funding and operational mechanisms.

3.1 Proposed Management Structure

3.2 ICT Board/ Steering Committee

The ICT Board Chairman is appointed by Vice Chancellor. Other members include:

i . The Registrar or a representative of the Registrar

ii. Heads of Faculties

iii. HOD, Computer Science

iv. SRC Representative

v. Head of ICT Services Unit

vi. Librarian or his/her representative

In attendance:

vii. Assistant Registrar appointed by the Registrar, as secretary

viii. Webmaster

The Committee shall be responsible for providing a high-level mechanism to:

i. Monitor and control the progress of all activities arising from the implementation of the University's ICT Policy.

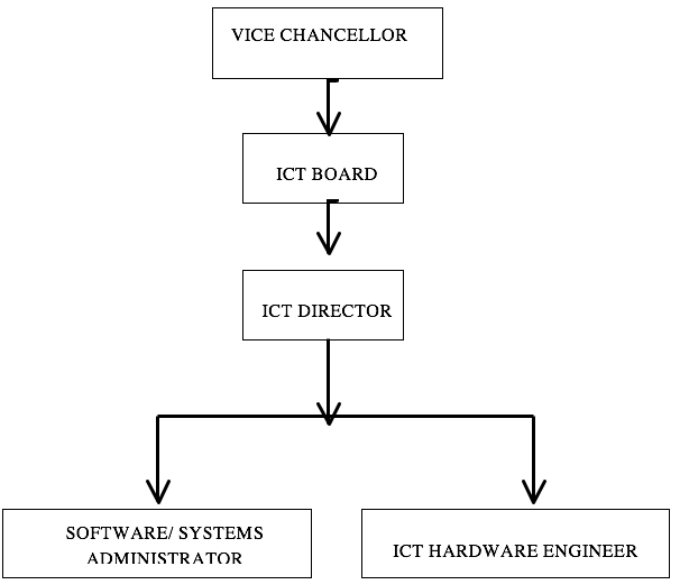
ii. Allocate resources according to the agreed master plan.

iii. Budget for the cost of management, operations, maintenance and expansion through the University budget.

iv. Recommend proposals for cost-recovery and cost-sharing.

v. Determine /approve ICT Policy adjustments arising from technology trends or new visions and strategies.

vi. Design strategies to raise revenue for a sustainable maintenance systems.



3.3 ICT Services Unit (ICTSU)

The University shall adopt an ICT management model with service deployment at both the centralized and decentralized levels to offer complimentary support services across the units. It is the University's policy to provide adequately skilled and resourced ICT management structures and procedures to ensure timely access to support services by all end-users.

The ICTSU shall implement policies; establish procedures and practices that shall directly affect academic and administrative units of the University.

Due to the crosscutting nature of their tasks, the Head of the unit shall report directly to the Rector on regular basis. Highly Trained personnel shall be profiled and recruited to perform specialised tasks at all times.

3.4 General Information Resource Ownership

All ICT resources for official use shall be owned by the p University. It is the University's responsibility to ensure sustainable use and maintenance of ICT resources.

3.5 Hiring of External Expertise

The University is allowed to hire certain support services from external professional providers in consultation with ICTSU/Board, if cost-effective and where the expertise involved is not available in the University. External consultants shall abide by this policy document, as well as industry best practices, Legal and Regulatory regimes at all times.

3.6 Service Level Agreement

A Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the

service provider. This can only be a legal binding formal contract.

The SLA records a common understanding about services, priorities, responsibilities, guarantees and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service such as billing. In some contracts penalties may be agreed in the case of non-compliance of the SLA. It is important to note that the 'agreement' relates to the services the customer receives, and not how the service provider delivers that service. Service levels of the ICTSU shall be determined between the University and the relevant Service providers in line with the ICT Services/systems provided and related service level requirements.

3.7 Sustainability of ICT resources

The key recurrent cost elements that should be considered include;

i. Cost of bandwidth.

ii. Cost of maintenance of equipment and applications.

iii. Recurrent cost of software licenses (application for the main information systems, specialized applications, database platforms, and desktop applications).

iv. Cost of replacement of equipment (e.g. a computers must be replaced when there is the need).

v. Emoluments for ICT professional that provide special support service to the University.

vi. Budgetary allocation shall be made for the Department of ICT.

The University shall develop and institutionalize relevant strategies for funding, policy drivers and human skills. Relevant internal and external stakeholders and development partners shall be engaged to provide solutions for sustainable ICT resources.

3.8 ICT Fee

The University Management in consultation with the Student Representative Council (SRC) shall put in place a ICT fee payable annually by each student to ensure that ICT services and systems can be expanded and sustained at the level compatible with the University's needs.

3.9 Collaborations

The University shall continue to improve its internal ICT infrastructure and systems to leverage research and academic collaborations with other institutions of Higher Education, in content creation. This shall further improve affordability of scarce ICT resources and add value through shared resources. Internally, ICTSU shall collaborate with designated ICT academic and research units on a non-profit basis, for the development of sustainable ICT solutions.

4.0 DATA COMMUNICATIONS INFRASTRUCTURE

The ICT infrastructure is conceived as comprising of three major components: - the data communication network; A Network Operations Center (NOC); computing resources for the users.

4.1 The Data communication infrastructure

The data communication infrastructure provides the essential links between users of information and sources of information. The University shall establish a University wide data communica-

tion network consisting of the following building blocks;

i. A data backbone inter-linking all buildings for each University campus. The following functional requirements shall guide the technology option used: - Highest speeds, reliability, efficiency, ease of maintenance and sustainability.

ii. Inter-campus connections between the different sites of the University. Options for either owner or leased links shall be considered whenever a procurement choice is to be made.

iii. Individual Local Area Networks for all administrative and Academic buildings at each University campus. Every staff shall have provision for network access at a work space and every student computing facility shall be linked to the backbone

iv. Infrastructure for wireless access within students' hall of residence on the various campuses.

The University shall promote ubiquitous and equitable access to ICT resources for students and staff to the network through the establishment of network infrastructure in all work areas of students and staff.

4.2 The Network Operations Center (NOC)

The NOC shall be the home for all back-end servers and related equipment that provide the hardware platform on which all the central network services shall be run. It shall also be the major switching for the data communication network. The University shall establish the Network Operations Center (NOC), specially designed with cooling, uninterruptible power supply, backup-facilities, physical protection, and smart access control. To assure a quick turn-around time in case of disasters, a duplicate of the

NOC, i.e. a Disaster Recovery Center (DRC) shall be established as at a remote location. It is the University's policy that all services that are common/shared by the whole University community are centrally hosted in the NOC.

4.3 User Computing Resources

These consist of computers and related accessories the University community uses to access the various network services and to facilitate work. Every University User shall have adequate computing time to carry out his/her work. Computing resources are categorized between the two groups.

4.4 Department Computing Resources

The University shall provide computing resources to enhance Department operations. The University shall provide a computer at Head of Department's / Dean's/Management member's desk and that of the Administrative Staffs (if required).

4.5 Student Computing Resources

The University shall provide computer laboratories for each School/Faculty and departments which offer programmes that use computers extensively in their course (e.g. ICT programme) The University shall also explore possibilities of loan schemes for student ownership of computers to ease the load on these pool facilities.

For both categories of users, wireless network access shall be made available within various campus locations where users can comfortably access ICT services. Particular focus shall be on computer laboratories and libraries.

4.6 Electronic Mail Services

Electronic mail (E-mail) services provide users with the means to exchange digital messages using a store and forward mechanism. Electronic mail systems accept, forward, deliver and store messages on behalf of users, who only need to connect to the e-mail infrastructure for the duration of message submission to, or retrieval from, their designated server.

Electronic mail services depend on correctly functioning Network support services, especially the Domain Name System services which enable the back-end servers to locate other e-mail servers and vice versa, and authentication systems that identify email users. It is the University's policy to provide each student and member of staff with an e-mail address under the official University domain name structure.

4.7 Access to Internet

Access to the Internet is one of the most valuable communication services for institutions of higher learning. It provides access to a wealth of information sources located on computer systems around the world. Like the e-mail service described above, the service relies on correctly functioning low level network support services. It is the University's policy to provide Internet access to all its students and staff to facilitate research and learning.

4.8 Web Services

Within the context of this policy, Web services shall provide facilities for storage of information formatted as web pages, and make such information accessible to the University community and the general public. The University web page shall publish information whose access shall not be restricted, and therefore shall be available to all users on the Internet. It is the University's policy to provide web services for the purpose of disseminating information within the University and to the rest of the Internet community.

5.0 MANAGEMENT INFORMATION SYSTEMS

The University shall harness the potential of ICTs to enhance services to staff and students. To this end, the automation of various management functions and processes through established integrated Management Information Systems shall ensure that the core category of the University stakeholders is provided with various management services in an effective and efficient manner. The focus of automation falls under two categories – Academic and Administrative. The Academic shall include - Library services and Teaching/Learning (E-learning). The administrative shall include - Human resource management, Academic Records Management, Financial Management, and Academic and Research systems.

The University shall improve its academic and research work through information systems that support the efficient management of academic and research processes. These shall include e-learning, the library and academic support applications.

5.1 Library Information System

To create an environment in the library for the use of Information Technology, the University shall provide the library with a Library Information System that shall support its administrative and management processes. This shall ensure circulation control, catalogue maintenance, sharing of resources among libraries at different locations, on-line catalogue access, Statistical reporting and management of information.

5.2 Administrative Systems

The University shall automate its core administrative functions by establishing three integrated information systems targeted to address the Finance, Human Resource and Academic Records Management functions.

5.3 Academic Records Information System (ARIS)

The University shall ensure that student academic records are efficiently and effectively managed through the establishment of Academic Records Information System (ARIS). The system shall provide for proper storage, retrieval and manipulation of student personal, academic, admission and financial data. This shall among others aim at reducing on the registration queues, standardizing the academic structure, eliminating duplication of academic courses, enabling automated application and admission as well as managing study records safely and efficiently.

5.4 Financial Information System (FINIS)

The University shall ensure the effective and efficient management of its financial data through a Financial Information System, which shall enable the automated collection, storage and analyzes of University financial data. The Information System shall support and improve Cash collection, debt management, foreign aid management, budgets preparation, ledgers management, accounts payable and receivable including other accounting functions. This shall enable the University to make good financial management decisions in budgeting and financial forecasts saving the University money.

5.5 Human Resource Information System (HURIS)

A Human Resource Information System shall be implemented in the University to enable the effective and efficient management of the human resource functions through capturing of personnel information and manipulating it to handle the administrative needs of the Human Resource Management Unit. This shall enable the University engage in efficient and accurate planning, recruitment of employees, orientation, training, appraisal, motivation, remuneration, salary administration and pension fund administration through use of the data that is captured by the information system.

6.0 SOFTWARE

These shall include the operating systems and applications that are used on a typical desktop computer/laptop. The University discourages the use of non-licensed software and aims at ensuring that only legal software is installed on its computers. The University shall endeavour to provide and maintain licensed software applications for all its users using a centralized procurement approach. The software shall be configured and used in accordance with the license terms and conditions as set out by the copyright holder.

6.1 Standardization of the operating environment

Standard Operating Environment (SOE) is a specification for a standard computer architecture and software applications that is used within the University. This ensures that the risks of copyright breaches or license non-compliance are addressed in addition to improving reporting and reducing the total cost of ownership by increasing efficiency and productivity.

University clients who acquire and/or install software are responsible for ensuring that they do so in accordance with the relevant IRM procedures. In all instances clients must ensure that software is used in accordance with the license terms and conditions as set out by the copyright holder.

6.2 Software Acquisition

The acquisition of any software shall be done in consultation with the central ICTSU. At the time of acquisition, the University shall consider the most appropriate option among the following with the guidelines as defined therein.

6.3 Software development

For crosscutting software, the ICTSU shall have to be consulted at all stages of development so as to meet the required standards. For department specific software the development shall be done in consultation with ICTSU. In either case, development of software shall be done in consideration of cost and human resource to ensure optimisation of effort. Existing systems shall be extended/ fixed/upgraded where possible rather than source new solutions.

6.4 Off-the-shelf software (Propriety Software)

For crosscutting software, identification of software, procurement and modification to suit University specific needs shall entirely be the responsibility of the ICTSU in consultation with Management. Procurement of department specific software shall be the responsibility of the respective department but shall be done in consultation with the ICTSU.

The ICTSU shall advise, conduct an evaluation of the desired system with the department and vendor, and shall provide an assessment detailing all of the aspects of the evaluation. The Faculty or department or unit shall then have all of the necessary information to make an informed decision as to whether they want to acquire the system.

6.5 Free and Open Source Software

Open source software (OSS) is that for which the source code and related rights are freely available to the public domain for use, change, improvement of the software, and redistribution in modified or unmodified forms. The University encourages the use of such software where applicable as it typically provides a sustainable solution in addition to developing technical capacity

6.6 Software Ownership

For developed software, ownership refers to authority over the source code. For propriety software, it refers to the ownership of the licenses that come with the software. Titles to computer software and software support materials developed by department/ unit, and students (through final year project) in the University shall belong solely to the University

7.0 SECURITY

The University shall meet its goals of protecting the confidentiality, integrity and availability of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

7.1 Access rights

The University shall, from time to time, establish access levels, rights, privileges, obligations and sanctions consistent with the University Information Policy, aimed at enabling easy access to corporate data and information needed for the different roles of the University community, while assuring the integrity of such data and information and respecting the privacy of individuals.

7.2 Antivirus Solution

The University shall ensure secure computer working environments by providing protective software (antivirus) designed to detect, remove and defend all University computers against malicious software or malware or viruses. The University shall establish appropriate guidelines for usage of the antivirus in consultation with the ICTSU.

8.0 MANAGEMENT OF INSTITUTIONAL DATA

Institutional data refers to all data created, collected, maintained, recorded or managed by the University and/or agents working on its behalf, which satisfy one or more of the following criteria:

i. The data is relevant to planning, managing, operating, or auditing a major administrative function of the University;

ii. The data is referenced or required for use by more than one organizational unit;

iii. The data is included in an official University administrative report;

iv. The data is used to derive a data element that meets these criteria;

This data can be contained in any form, including but not limited to documents, databases, spreadsheets, email and web sites; represented in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination there of; communicated in any form, including but not limited to handwriting, printing, photocopying, photographing, and web publishing; and recorded upon any form, including but not limited to papers, maps, films, prints, discs, drives, memory sticks and other computing devices.

8.1 Types of Institutional data

i. Research Data – refers to all outputs of creative work undertaken on a systematic basis in order to increase the stock of knowledge and information.

Examples include research publications (books, book chapters, journal, articles, conference publications, thesis and

dissertations), project/annual reports; planning documents (policies, strategic plans).

ii. Library Data – refers to data, which contain information on University library profiles such as subscribed journals, available print collections (books, serials and references), available special collections (photos, music, archives).

iii. Academic Data – refers to data, which contain information on University academic profiles such as courses/curricula, enrolment, degree/transcript, course/examination timetables and alumni.

iv. Student Data – refers to information relating to student characteristics (course and residence registration, academic performance, financial status) and student demographics (region, age, sex, religion)

v. Human Resource Data – refers to data, which contain information on the human resource profile of the University such as establishment; staffing level; procedures and manuals; benefit schemes and beneficiaries.

vi. Personnel Data – refers to information relating to staff characteristics (qualification, rank, pension accrued, compensations, salary etc) and staff demographics (region, age, sex, religion, marital status, department etc).

vii. Financial Data - refers to data, which contain information on University financial profiles such as revenue, expenditure, budget, assets and facilities.

viii. Protected Data - data that require a higher level of classification than public data such as Confidential and Restricted

Data;

ix. Confidential Data -Data categorized as 'Confidential Data' may be data that would not be made available or disclosed to unauthorized individuals, entities or processes for legal and or business reasons.

x. Restricted Data - data to which access is subject to special controls for reasons of security or safeguarding the data.

xi. Public Access - Data which at the absolute discretion of the University, are determined to be a matter of public record and can therefore be made freely available without restriction are categorized as 'Public Access'.

8.2 Roles and Responsibilities

The University shall ensure that roles and responsibilities associated with each institutional data are well defined. Roles shall be defined to include;

8.2.1 Data Owner – The University owns official information/ data under its jurisdiction.

8.2.2 Data Custodian - a University unit or employee responsible for the operation and management of systems and servers which collect, manage, and provide access to institution's data. Thus, the Head of ICTSU, including its staff, is responsible for managing the server that houses the academic data (ARIS).

8.2.3 Data User - Data Users are individuals who access University data to perform their assigned duties and for purposes provided for by this policy. Data Users are responsible for protecting their access privileges and for the proper use of the data they access.

The University shall ensure that information relevant for tactical and strategic needs of University management and top executives is provided in a timely and easy to access way. The University shall therefore, promote and support the development of high level reporting applications that consolidates data from across all institutional databases using data mining and/or other approaches.

8.3 Data Security

Institutional Data must be safeguarded and protected according to approved security, privacy and compliance guidelines, laws and regulations established by the University and/or the country. Permission and access to institutional data shall be granted in accordance with defined access and use policies and procedures determined by the Data owner.

The ICTSU shall develop and implement an appropriate backup and restoration policy, a business continuity plan and information security policies to ensure protection, integrity and reliability of all institutional data.

The University shall promote the development of a centralized system of authentication that ensures users of the University's information technology resources and associated data are correctly identified, authorised and authenticated before access to the corresponding systems and resources is granted.

The University shall ensure that whenever certain portion of a given institutional data is generated and maintained by an external party – example students' results; fees payment at respective banks - appropriate procedures and guidelines are developed to guide the exchange of such data.

9.0 INFORMATION TECHNOLOGY STANDARDS

The Information Technology Standards Policy lists all technologies supported by the organization and serves as a guideline for all technology purchases and use decisions, including hardware, software, peripherals, and network components. The primary goals of developing and implementing such a policy are:

i. To ease purchasing decisions by pre-evaluating and pre-approving technology solutions.

ii. To reduce training and support costs and create economies of scale by narrowing the number of technologies and products used.

iii. To ensure integration and interoperability between technologies.

iv. To set parameters for future technology innovation and development.

The following standard technologies were selected based on prevalence in the organization or in the case where two or more competing technologies previously existed on an assessment of relative quality and performance as dictated by business needs.

9.1 Hardware Standards

The following guidelines for standards are based on the current technology available combined with the current needs of the end-user today. The primary considerations for each specification (desktop, printing, portable computing) are;

1. Ease of connectivity to the University network.

2. Consistent performance of all integrated components in our network environment.

3. Industry leader with an established track record in manu-

facturing, sales and service.

4. Successful in-house experience with the chosen product and configuration.

5. Serviceability by the IT Department.

6. The machine has a minimum campus lifetime of four years .

There shall be standard specifications for newly procured computers which shall be updated as need be.

10.0 UNIVERSITY COMPUTER EQUIPMENT

10.1 Replacement of University Computer Equipment

All University computer equipment shall be replaced as and when required. ICTSU staff shall periodically meet with Departments to check on computers that need to be replaced.

The goals of the replacement plan are to:

i. Ensure that appropriate computing resources are available in libraries, laboratories, and offices to support the mission of the institution;

ii. Ensure that each faculty and staff member who uses computing resources in his or her position has a computer of sufficient capability to fulfill his/her responsibilities;

iii. Implement minimum standards for computing equipment on campus, and encourage planning, cost-effective installation of new equipment and disposal of old equipment.

The University shall maintain a central inventory of ICT equipment. Any ICT equipment procured shall be added to the central inventory. At the time new equipment is recorded in the inventory, if there is a request for replacement of any equipment by a Department/Unit it shall be assigned accordingly. Replacement of such equipment is by a special request to the Rector and old equipment shall be sold for residual values through Takoradi University official salvage plan.

10.2 Grant Funded Equipment

Departments pursuing grants for computing equipment should discuss their plans with the Rector in consultation with the ICT Officer, and Finance Office as part of the budgeting process. Computing equipment that is acquired under grant shall be recorded in the inventory.

Departments that may have access to research funds under certain conditions may be used to buy ICT equipment for office use but the equipment shall belong to the University. Such equipment should be ordered through the University purchasing process and shall not normally be upgraded or replaced by the University, except through further use of research funds.

10.3 Printers and Other Peripheral Equipment

The University provides networked printing locations for workgroup clusters. Individual desktop printers shall be provided for offices. Other peripheral pieces of equipment such as scanners shall be provided in clustered locations as well as required individual offices. Since these pieces of equipment are usually used intermittently, clustering allows sharing of specialized technical resources.

10.4 Responsibility for Equipment

Each employee is responsible for taking reasonable safety precautions in regard to Takoradi University-owned computer equipment. Employees shall be held responsible for damage to such equipment arising out of their negligence or intentional misconduct.

11.0 ICT PROCUREMENT

This document describes how the institution deals with the procuring of ICT related hardware and software. This policy must be based on an agreement between ICTSU, Procurement, Finance and Audit and must be approved by the Vice Chancellor.

In case of differences in opinion or deadlock that may arise between the ICTSU and the procuring department, appeals could be registered with the Vice Chancellor, who is the final authority. Central servers and personal computers shall be replaced as and when required depending on performance, increase in demand, obsolescence rate and application software requirements. The ICT Centre in conjunction with University Management shall develop a replacement strategy to meet this obsolescence. The disposal of obsolete equipment shall be carried out in accordance with the existing government guidelines.

12.0 RESOURCE DISTRIBUTION

The purpose of this section is to ensure that proper procedures are followed in distributing or assigning ownership to specific ICT systems. This shall prevent the unauthorized or inadvertent disclosure of sensitive information pertaining to specific department/unit. (Example, Finance, Personnel etc.)

12.1 Guiding Principles

1. All ICT facilities shall remain the property of the University. Computer laboratories shall belong to ICTSU. Requests for ownership for specialized facilities shall be made to the ICT Board through the office of the Vice Chancellor

2. Subject to resource availability The University shall provide computers in every staff room and in the long term on every lecturer's desk. This shall be extended to all support staff that need computers to perform their duties. Other support staff whose tasks require less use of the computer shall be provided with shared central facilities.

12.2 Access to Network facilities

1. There shall be only one network point per office. Where space is to be occupied by several staff members, the affected department shall be expected to identify this requirement at the time of network design. Any modifications to the University network shall be done in consultation with the ICT Officer.

2. The University shall develop facilities to meet the needs of student and staff ICT resource requirements. However, techniques such as access control, access quota etc. shall be used to ensure equitable access to ICT resources.

13.0 GENERAL RESPONSIBILITIES OF ICTSU

1. The ICTSU bears the responsibility for compliance with all policies, guidelines, procedures and standards developed and adopted in consultation with the University management structures for acquisition, implementation, documen-

tation, and delivery of information technology.

2. The ICTSU shall be responsible for delivering data, video and related online services by designing, installing, and maintaining the institution's network infrastructure. The ICTSU shall also provide access to information, systems, and services at other University campuses by providing inter-network connectivity.

3. The ICT board shall advice and review matters related to instructional, research, and administrative applications of technology.

4. The University management, staff and students share the responsibility for effective ICT resource management. These responsibilities include those directed by University policies and procedures for secure, hospitable, equitable, and ethical use of IT resources.

5. The ICTSU shall be responsible for establishing and maintaining physical and logical security of central servers, communications network, and data for which it is the custodian.

6. The ICTSU shall also be directly or indirectly be responsible for the maintenance of all ICT systems.

7. The ICTSU shall be responsible for instituting and monitoring appropriate access control mechanisms for systems it administers. Access to these systems shall be granted by issuance of an individual user login identification, password protection and appropriate usage restriction, following a written request from the office responsible for data requested.

14.0 REPAIR OF COMPUTER EQUIPMENT

All University computer equipment is maintained in-house. If a hardware problem is suspected the user shall call the ICT support staff during normal business hours for assistance. If hardware service is indicated, arrangements shall be made with the technician.

14.1 Personally Owned Equipment

ICTSU shall provide repairs for personally owned computers. Computers are repaired at a cost rate established by the University. There is a minimum charge for examining the equipment if repair is not needed. Equipment must be delivered to the ICTSU during regular business hours. ICTSU shall be available each day between 9 am and 5 p.m. to receive equipment or by special arrangement. Payment for the repairs must be made by cash, check, or money order when the equipment is picked up.

15.0 IT ASSET DISPOSAL

Takoradi University's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, databases, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and Takoradi University's upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to company-approved methods.

15.1 Definitions of Disposal terms

Non-leased refers to any and all IT assets that are the sole property of the University; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.

Disposal refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and

environmentally sound means.

Obsolete refers to any and all equipment over 10 years old and/or that which no longer meets requisite functionality.

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

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

15.2 Guidelines for Disposal

Disposal procedures of all ICT assets and equipment shall be managed and coordinated by ICTSU. ICTSU is also responsible for backing up and then wiping clean of institution data on all IT assets slated for disposal, as well as the removal of institution tags and/or identifying labels. The ICTSU is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills.

15.3 Practices

Acceptable methods for the disposal of ICT assets are as follows:

i. Auctioned to staff.

ii. Donated to Students/ Basic and Second Cycle Institutions.

iii. Auctioned as scrap to a licensed dealer.

iv. Used as a trade-in against cost of replacement item.

v. Reassigned to a less-critical business operation function.

vi. Donated to schools, charities, and other non-profit organizations.

vii. Recycled and/or refurbished to leverage further use (within limits of reasonable repair).

viii. Discarded as rubbish in a landfill after sanitized of toxic materials by approved service provider.

15.4 Duties of ICTSU with respect to Disposal

It is the responsibility of Staff of ICTSU with the appropriate authority to ensure that ICT assets, equipment, and hardware are disposed according to one or more of the methods prescribed above. It is imperative that any disposal performed by the University is done appropriately, responsibly, and ethically, as well as with company resource planning in mind.

The following rules must therefore be observed:

1. Obsolete ICT Assets: As prescribed above, "obsolete" refers to any and all computer or computer-related equipment over 10 years old and/or equipment that no longer meets requisite functionality. Identifying and classifying ICT assets as obsolete is the sole province of ICTSU. Decisions on this matter shall be made according to the University's purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).

2. Reassignment of Retired Assets: Reassignment of computer hardware to a less-critical role is made at the sole discretion of ICTSU

It is, however, the goal of the University to – whenever possible – reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures.

3. Trade-Ins: Where applicable, cases in which a piece of equip-

ment 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 IT asset against the cost of the replacement. The University's Purchasing and Procurement manager or IT Asset manager shall assume this responsibility.

4. Income Derived from Disposal: Whenever possible, it is desirable to achieve some residual value from retired or surplus IT assets. Any and all receipts from the sale of IT assets must be kept and submitted to the Finance Department. Income derived from sales to staff, the public, or students must be fully receipted and monies sent to theUniversity's Finance Department. Sales to staff should be advertised through the company intranet or via e-mail.

5. Cannibalization and Assets beyond Reasonable Repair: The ITC Officer is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as such should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the organization. The IT Department shall inventory and stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means shall be sold to an approved scrap dealer or salvaging company.

6. Assets decommissioning: any hardware that is slated for disposal shall be wiped clean of company data. The University's ICTSU shall assume responsibility for decommissioning this equipment by deleting all files, company-licensed programs, and applications using a pre-approved disk-sanitizer. This sanitizer must completely overwrite each and every disk sector of the machine with zero-filled blocks. In addition, any property tags or identifying labels must also be removed from the retired equipment.

7. Harmful Substances: Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill as rubbish. The ICTSU may perform this action itself using government-approved disposal methods, or hire an accredited disposal company specializing in this service. No matter what the route taken, the removal and discarding of toxins from the University equipment must be in full compliance with local and national laws.

8. Donations: IT assets with a net residual value that are not assigned for reuse, discarding, or sale to employees or external buyers, may be donated to the University approved schools, charity, or other non-profit organization. All donations must be authorized by the University and all donation receipts must be submitted to the Finance Department for taxation purposes.

16.0 DATA BACKUP

Data is one of the University's most important assets. In order to protect this asset from loss or destruction, it is imperative that it shall be safely and securely captured, copied, and stored. The goal of this document includes a policy that governs how and when data residing on University computers shall be backed up and stored for the purpose of providing restoration capability. In addition, it shall address methods for data restoration

16.1 Backup Schedule

There shall be monthly full backup and weekly differential backup, which shall be verified periodically.

16.2 Data Storage

It is the University's policy that ALL University data shall be

backed up according to schedule. This includes any University documentation (i.e. reports, contracts, etc.), e-mails, applications/ projects under development, Web site collateral, graphic designs, and so on, that reside on end-user workstations.

1. Office Users: the University data, especially works-in-progress, should be saved. This ensures that data shall be backed up when the servers are backed up. If data is saved on a workstation's local drive, then that must be backed up every week onto storage media.

2. Remote/Mobile Users: Remote and mobile users shall back up data as "Office Users" above.

16.3 Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential that the IT Department regularly test its ability to restore data from the storage media or network drive. As such, all storage media must be tested at least once every month to ensure that the data they contain can be completely restored to end-user workstations/server.

Data shall be restored from a backup if:

i. There is an intrusion or attack.

ii. Files have been corrupted, deleted, or modified.

iii. Information must be accessed that is located on an archived backup.

In the event that an end-user requires or desires a data restore, the following guidelines shall be adhered to;

1. The individual responsible for overseeing backup and restore procedures is the IT Officer. If a user has a restore request,

they can contact ICTSU by calling, sending an e-mail, or filling out and submitting a request form.

2. Mobile and/or remote users shall likely be carrying their backups with them. In the event that a restore is needed, the user shall contact the University ICTSU. The ICTSU shall walk the user through the restore procedure for their mobile device.

3. In the event of unplanned downtime, attack, or disaster, the University's full restoration procedures shall take place.

4. In the event of a local data loss due to human error, the end-user affected must contact the ICTSU and request a data restore. The end-user must provide the following information;

    i. Name.

    ii. Contact information.

    iii. Name of file(s) and/or folder(s) affected.

    iv. Last known location of files(s) and/or folder(s) affected.

    v. Extent and nature of data loss.

    vi. Events leading to data loss, including last modified date and time (if known).

    vii. Urgency of restore.

5. Depending on the extent of data loss, backup tapes and storage media may both need to be used. The timing in the cycle shall dictate whether or not these tapes and/or other media are on-site or off-site. Tapes and other media must be retrieved by the server administrator or pre-determined replacement. If tapes and/or other media are offsite and the restore is not urgent, then the end-user affected may be required to wait for

a time- and cost-effective opportunity for the tape(s) and/or other media to be retrieved.

6. If the data loss was due to user error or a lack of adherence to procedure, then the end-user responsible may be required to participate in a tutorial on effective data backup practices.

17.0 EMPLOYEE DEPARTURE CHECKOUT CHECKLIST

This checklist explains the employee departure checkout process. Follow these steps for any employee departure, whether voluntary or involuntary. This checklist assumes that appropriate written notification of pending departure has either been supplied by the employee in the event of resignation, or shall be supplied to the employee in the event of termination.

i. Notify the appropriate personnel in ICTSU in advance that an employee shall be departing so that they can take appropriate security measures. If the employee is being terminated, notify ICT Officer that all of the employee's accounts (network, e-mail, and voice) shall need to be deactivated at a particular date and time. Ideally, deactivation should take place while the employee is being notified of his or her termination.

ii. List in advance any equipment and files that should be in the employee's possession and must be returned.

iii. Conduct an exit interview. At this interview, the following must be addressed.

iv. Review final compensation procedures and timeframe, including payout of any vacation pay accrued.

v. Review termination date of any and all benefits, and any provisions for temporary extension of benefits.

vi. Review any confidentiality and non-disclosure requirements.

Remind employee that all files and documents are property of the University and cannot be destroyed, removed, modified, or copied without approval from the direct supervisor.

vii. Ensure return of all company property to the employee's supervisor, or make arrangements for its immediate return. The University property includes all keys, access cards, identification cards, credit cards, parking passes, tools, books, reference materials, software, and equipment (such as laptop computers, personal digital assistants, pagers, and cell phones).

viii. Gather and/or confirm the employee's forwarding information, including home address and e-mail address (if appropriate).

ix. Has the employee disclosed all usernames and passwords to all accounts and/or applications to the employee's supervisor for records management and redistribution purposes?

x. Review the status of any and all projects or work in progress.

xi. Has the employee disclosed the location of key work-related documents and records?

xii. Have all work-related computer files transferred to ICTSU for secure review by the departing employee's successor or supervisor. These files shall be deleted, stored, or forwarded to the appropriate University staff.

xiii. Arrange for return of personal print and computer files to the employee

xiv. All personal items, such as plants and family photos, must be removed from the employee's work area by the employee as close as possible to the time of employee departure. Under stressful circumstances, arrangements can be made for

employees to clear out their personal items during off hours.

xv. Arrange for the departing employee's e-mail and phone calls to be temporarily forwarded to the employee's supervisor.

18.0 INTERNET / INTRANET USAGE

Like many other organizations, Takoradi University has provided Internet connection because the internet plays an important role in education, especially research activities. The management of the institution recognizes that the provision of Internet access to global electronic information resources on the World Wide Web shall tremendously assist both teaching and non-teaching staff as well as student in obtaining work-related data and technology.

18.1 Accessing the Internet

The following are prohibited in accessing the internet provided by the University;

1. Participating in illegal music sharing using peer-to-peer software (examples are, imesh, napster, etc).
2. Downloading music and movies from the internet.
3. Sending or posting discriminatory, harassing, or threatening messages or images.
4. Using the institution's time and resources for personal gain
5. Stealing, using, or disclosing someone else's code or password without authorization.
6. Sending or posting messages or material that could damage the institution's image or reputation.
7. Participating in the viewing or exchange of pornography or obscene materials.

8. Sending or posting messages that defame or slander other individuals or the University community.

9. Sending or posting chain letters, solicitations, or advertisements not related to the University's business purposes or activities.

10. Using the Internet for political causes or activities, religious activities, or any sort of gambling.

11. Sending anonymous e-mail messages.

12. Engaging in any other illegal activities.

19.0 COMPUTER SECURITY

Information processing, management and security whether manual or automated, are fundamental requirements for the institution's day-to-day operations.

19.1 Access to computing equipment

1. All computing equipment shall have reasonable physical security in place (i.e. reasonable measures to prevent theft). Any action or attempt by a user to subvert or disrupt the functioning of any computer equipment is prohibited.

2. Relocation of any computer resources from any of our premises shall be completed in consultation with the ICT Officer. In the case of laptop computers, the department or individual to whom this equipment is assigned is responsible for an appropriate process to control its movements.

3. No person or persons shall, by any deliberate act, jeopardize the integrity of the computing equipment, its systems, programs or other stored information.

4. Each user is responsible for maintenance of files on their account. It is necessary for the user to review various documents that exist and remove those that are no longer required.

5. Users must not install software on to the hard drives or any of the computer networks without the expressed permission of the ICTSU

6. ICTSU Staff shall be responsible for backups of data on the institutions -wide servers. All data on workstation hard drives or other media are the responsibility of the user.

7. Users must not knowingly install a virus on to the institution's computers or networks.

8. Anti-virus protection tools shall be installed and upgraded / active on all the University's computers and networks

9. Establishment of security perimeters around server rooms and sensitive areas by walls, self-shutting doors, lockable doors, alarms and security curtains.

10. Computers and major components shall be marked with identifying information, including the institution's name, location of computer and user.

11. Serial numbers of computers and components shall be logged so that they can be easily identified and recovered if stolen.

12. Encourage staff to pick up documents immediately from central printers, fax machines and copiers.

13. Set up secured printers for confidential information.

19.2 Computer Security Responsibilities of ICTSU

1. The ICT board shall overseer of the establishment and implementation of all ICT policies, procedures and guidelines, and other related security policies.

2. The ICTSU shall be responsible for ensuring reliable and secure ICT systems, in accordance with industry best practice.

1. The ICTSU shall establish and provide physical and logical security of central computing facilities; the other departments shall be responsible for the same within their domain.

2. The ICTSU has the additional responsibility of establishing a comprehensive disaster recovery and emergency procedures for all ICT resources. All users and managers of sub-systems shall feed into this wider plan.

3. Users are responsible for familiarizing themselves with all policies, procedures and standards relating to information security, and are responsible for appropriate handling of raw or interpreted data.

20.0 OFFICIAL ELECTRONIC MAIL USAGE

Electronic messaging systems are alternative to paper-based letters, memos and notices, etc.

They provide a medium for transfer of information and can be used to support teaching, research, support services and administrative activities. The purpose of this Policy is to ensure that the University community is informed about the applicability of policies of electronic mail.

20.1 **E-mail Access**

1. A formal authorization process shall be followed by all Departmental Heads for allocation of official email accounts to staff.

2. No email attachments having .vbs / .exe /.api or any other file of executable nature shall be exchanged or downloaded by students or staff without approval.

3. No user shall exchange proprietary data over email, without prior authorization from the information owner.

4. Users shall not indulge in any communication of information pertaining to religion, politics or other personal opinions, which are not job-related.

5. The University electronic mail services shall be limited primarily to University students and staff.

6. No user shall exchange any obscene messages or any information that can be deemed to be pornographic in nature or such that it is sufficient to affect the image of any persons within or without the organization.

7. Users shall exercise utmost caution when sending any email from inside the institution to an outside network.

8. Mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized to do so. Where appropriate, a disclaimer shall be included to explicitly show that the author is not representing the University. The essence of the disclaimer must be: "These statements are my own, not those of the University".

9. Users shall not feign an identity. However, recipients of

electronic messages must be aware that the identity of the sender may/may not be authentic. Senders must be aware that delivery of messages cannot be fully guaranteed.

10. The email services shall not be used for purposes that could cause excessive strain on any ICT facilities. No 'junk' mail shall therefore be sent using the institutions electronic mail systems. Junk mail includes, but is not restricted to chain letters, advertisements, and "spam", exploiting listeners etc.

11. Transport and Storage of Messages: Electronic mail systems should be considered a transportation mechanism and should not be used for long-term storage or archive. Each user shall be allocated a specified in-box quota.

20.2 **Email User Responsibilities**

1. The University Community are encouraged to use electronic mail, but are expected to do so in a manner consistent with the University's mission. The use of the messaging systems commits individuals to all applicable institutional ICT policies and guidelines.

2. The University employees have additional responsibilities by virtue of their access to a variety of institutional data. The employees shall obey applicable rules and regulations regarding data use and information security.

3. Special care must be taken to ensure that a distinction is made between personal and/or casual communication and official University communication.

4. The ICTSU is responsible for ensuring reliable, secure and efficient operation of the University's electronic messaging systems.

21.0 VIRUS PROTECTION

Computer virus programs pose a threat to the institution in terms of lost of data, productivity, compromised data integrity, unauthorized disclosure of sensitive information and potential negative impact to its reputation and credibility. All computer systems on any of the institutions network, or any other computer systems used for the University's business purposes is vulnerable to virus infection and must have current approved virus protection measures in place. This Policy defines the minimum level of virus protection required for all computer systems within this environment. This shall help to minimize exposure to computer viruses and its resulting problems.

21.1 Virus Protection Policy

Currently, the University's hall acquire antivirus from time to time to mitigate the virus attack. The most current available version of the anti-virus software package shall be taken as the default standard. All computers attached to the University's network shall have standard anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date. Any activities with the intention to create and/or distribute malicious programs onto the University network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the ICTSU immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the ICTSU. Any virus-infected computer shall be removed from the network until it is verified as virus-free.

21.2 Virus Prevention Rules

Recommended processes to prevent virus problems:

1. Always run the institutions recommended antivirus software installed by the ICTSU.
2. Ensure that you run the current version and install anti-virus software updates, as they are made available by the ICTSU.
3. Delete spam, chain, and other junk email without forwarding; in line with Internet Usage Policy.
4. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
5. Always scan a flash drives etc., from an unknown source for viruses before opening it.
6. New viruses are discovered almost every day. Periodically check the Anti-Virus Policy and the recommended processes list for updates.
7. For any updates of anti-virus software, always check with the ICTSU
8. DO NOT trust any other source for virus protection patches.
9. Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source. Delete these attachments immediately and then emptying the Trash.
10. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

11. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

12. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

13. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

14. Regularly update virus protection on personally owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

21.3 Virus Protection Responsibilities of ICTSU

The following activities are the responsibilities of the University ICTSU:

1. The ICTSU has the sole responsibility to provide antivirus system to ensure that all computer systems of the institution are protected.

2. The ICTSU is responsible for maintaining and updating this Anti-Virus Policy.

3. The ICTSU shall keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.

4. The ICTSU shall apply any updates to the services it provides that are required to defend against threats from viruses.

5. The ICTSU shall install anti-virus software on all Takoradi University owned and installed desktop workstations, laptops, and servers.

6. The ICTSU shall assist employees in installing anti-virus software according to standards on personally owned computers that shall be used for business purposes.

7. The ICTSU shall not provide anti-virus software in these cases.

8. The ICTSU shall take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT Department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

9. The ICTSU shall perform regular anti-virus sweeps.

10. The ICTSU shall attempt to notify users of Takoradi University systems of any credible virus threats via e-mail or telephone messages. Virus reports shall not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

21.4 Virus Protection Responsibilities for Departments and Users

The following activities are the responsibility of the University's departments and Staff:

1. Departments must ensure that all departmentally managed computers have virus protection that is in keeping with the standards set out in this policy.

2. Departments that allow employees to use personally-owned computers for official purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

3. Employees are to ensure that client versions of antivirus

are installed on their systems and are always updated.

4. All employees are responsible for taking reasonable measures to protect against virus infection.

5. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the University network without the express consent of the ICTSU.

21.5 Virus Protection Enforcement Policy

Any employee or student who is found to have violated the virus protection policy would be subjected to the Employee/Student Conduct Code and may be subjected to disciplinary action, up to and including termination of employment/school.

22.0 PASSWORD MANAGEMENT

This policy establishes the minimum requirements for generating and managing passwords used by operating systems, Database Management Systems, or applications on all systems owned by or operated on behalf of the institution. Passwords are an important aspect of computer security and must be handled with care. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the institutions entire network. As such, all users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

22.1 Passwords Usage

1. Passwords must never be written down or stored in an unprotected fashion.

2. Users must be able to change their own passwords periodically.

3. Each user is accountable and responsible for any action taken with that user's User ID or Username and password. No users of the University should ever share or divulge their password to anyone.

4. Passwords must be protected at all times during their lifecycle (from generation to storage, delivery, and usage), and measures must be taken to ensure no disclosure to any unauthorized person or entity.

5. Passwords used on central systems, for example, controlled application or servers for critical business etc. must be different from passwords used on external email accounts, external Internet services, and other systems not owned by the University.

6. Initial passwords must be protected during distribution to the end user and shall be handled as temporary passwords.

7. Temporary passwords must be changed immediately upon the completion of the assigned task.

22.2 Password Selections

1. Passwords complexity must be enabled using the capabilities provided by the specific technology being implemented. The complexity requirements must be documented. The complexity level must meet minimally the complexity rules in the password management standard.

1. The password length requirement for each technology must be chosen to mitigate the risks associated with known password length vulnerabilities and must be documented in a technology-specific security standard.

22.3 Password Expiration

1. Every technology that uses passwords for credentials in authentication protocols must implement password aging and password expiration mechanisms that address the known risks for the specific technology.

2. Accounts with elevated privileges must age and password must expire in a timeframe commensurate to the risk.

3. Passwords issued for temporary IDs, password resets, and locked out IDs must all be reset to expire immediately. The recipients of temporary passwords shall then be forced to change their passwords at their first login opportunity.

22.4 Password Transmission and Storage

1. Passwords must be encrypted when transmitted across any network.

2. Passwords must not be stored or used in clear text for the purpose of automating a login sequence.

3. Passwords must be stored in an encrypted format that is cryptographically secured for the known risks and specific technology.

4. Account lockouts must address known risks for the specific technology or protocol being implemented.

22.5 Password Uniqueness or Minimum Age of Passwords

1. A mechanism must be in place to prevent the reuse of at least the last two passwords.

2. A user must not circumvent the history mechanism in order to retain the same password.

3. On systems or applications where password uniqueness

is not available, parameters must be set to restrict password changes. The user must be restricted from changing the password for a minimum of 24 hours.

22.6 Password Hacking

Attempts to "break", "hack", "crack", cause disclosure, or otherwise determine any password singly or in aggregate must not be attempted by any means.

22.7 Password Display, Logging and Printing

The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties shall not be able to observe or subsequently recover them. Passwords must not be logged or captured as they are being entered.

22.8 Here is a list of "don'ts":

1. Don't reveal a password over the phone to ANYONE
2. Don't reveal a password in an email message
3. Don't reveal a password to the boss
4. Don't talk about a password in front of others
5. Don't hint at the format of a password (e.g., "my family name")
6. Don't reveal a password on questionnaires or security forms
7. Don't share a password with family members
8. Don't reveal a password to co-workers while on vacation
9. If someone demands a password, especially to a central computer system, refer them to this document or the

HOD. ICTSU

10. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system without encryption.

22.0 THE APPROPRIATE USE OF OTHER ICT RESOURCES

The Institution is committed to providing users with access to its ICT systems. Such access and utilization of facilities and services is however subject to certain rules, regulations and restrictions. The access imposes certain responsibilities and obligations, and is granted subject to the Institution's policies.

22.1 User Responsibilities to Other ICT Resources

1. Internet Users should engage in activities that consume large bandwidth such as video conferencing, large file downloads, music downloads etc. Such activities shall be restricted to off-peak hours (after 5:00 p.m. or during weekends), unless authorized by University's Management.

2. Every user and consumer of ICT services and equipment shall be responsible for the ordinary care, upkeep and maintenance of such service point or equipment.

3. Prudence and integrity shall be expected in the use, security and care of all ICT resources and information.

4. Pursuant to the above, the University management shall produce regulations that shall enhance user responsibility, prudence and professionalism on institutional ICT matters.

5. Generally, by using the University's ICT resources, each user accepts the responsibility for his/her behavior and all

activities on his/her User-led activities, and agrees to abide by the following principles:

a. To access only files and data they own, that are publicly available, or to which they are individually given access.

b. To comply with copyright license requirements for all software and other people's works. Users shall not make illegal copies of the software or other people's works, store any illegal copies of software in the University systems, or transmit them over University networks.

c. To refrain from performing acts that shall interfere with the normal operation of IT Systems. Such acts include, but are not limited to monopolizing systems, overloading networks, wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

d. Not to use computer programs or other means to obtain access to passwords or gain unauthorized access to information.

e. Not to engage in any activity that might be harmful to systems or any information stored on the University systems, e.g. propagating viruses, disrupting services or damaging files and software programs.

f. Not to use mail or other messaging services to harass or intimidate others.

g. Not to disclose their passwords to other people or allow other users (whether members of the University community or otherwise), to use their usernames and passwords.

h. Not to use the University systems for any form of personal or organizational gain other than the University's approved duties e.g. sales of forms, campaigns, etc.

i. Not to install or operate computer games on University-owned facilities for purposes other than academic activities.

j. To respect all rules, regulations, policies and procedures adopted by the University or applicable to University facilities such as computer laboratories, library, printer locations, open access areas, etc. and all efficiency-aimed instructions given by technical staff.

k. Not to attempt or assist any attempt to violate systems security or cause any part of the institution's ICT system to become impaired or inoperable, or gain unauthorized access or entry to ICT facilities or databases.

23.0 END USER SKILLS DEVELOPMENT

The University Policy in the broadest sense is to promote the deployment of ICT in all areas of education and research through creating technical and organizational preconditions. End users are the University employees and students who make use of the available ICT resources and they generally fall into two categories; students and staff.

End user skills have to be developed so that all users are able to:

1. Use ICT services and systems effectively and as independently as possible.

2. Contribute to the specification, design and implementation of ICT applications.

3. Be aware of the shared responsibilities for equipment, soft-

ware and data, and enforce an atmosphere of collective responsibility and system ownership.

4. Manage and control complex project oriented processes, like implementing University-wide infrastructure or information systems.

5. Establish and sustain effective, use of the available ICT resources for academic, administrative, or managerial tasks.

23.1 Basic ICT Skills

Students shall be ICT literate during their time at the University. The Computer Science Department shall develop a standard cross-cutting basic ICT skills course which should be adopted and administered by all University units. It is University Policy to ensure that all students take the Computer Literacy course at the first year of their training and shall provide with skills tailored to their specific academic programmes. Staff shall be trained on a continuous basis in order to build their ICT expertise and experience. This shall ensure that they are competent enough to use ICT resources and to keep abreast of the dynamic and ever changing nature of ICT in Higher Education.

The University shall provide training that is innovative and adapts to both the dynamic changes in ICT and changing staff training needs and caters for staff at different levels of expertise in order to build capacity. It is University Policy to train staff on a continuous basis in basic ICT skills and other skills relevant to their jobs and require that all new staff to be recruited possesses the relevant ICT skills for the jobs applied for.

23.2 Academic Specific Skills

Although the Quality Assurance Directorate is mandated to oversee the development of academic programmes in the Universi-

ty, each academic and research unit shall be required to develop progressive and continuous ICT courses that are tailored to their specific academic disciplines. This shall ensure that students apply ICT skills throughout their learning experience.

23.3 Administrative Skills

Staff shall be able to understand and use the core University administrative applications such as the Human Resource Information System (HURIS). The Human Resource Unit shall develop and implement training strategies that help staff to make use of all the functions provided by the applications.

23.4 Library Services

The University Library makes use of ICT to provide access to a wide range of electronic information from both University and external sources. The end users shall have the information literacy skills to effectively use the electronic information which include electronic journals, databases and other resources.

The University Library shall organize and conduct training that shall:

1. Create awareness about the wide range of available information resources
2. Equip users with skills for determining their information needs
3. Provide users with the ability to locate and retrieve relevant information
4. Enabling users to evaluate information and its sources
5. Facilitate users' understanding of ethical and legal issues sur-

rounding information use.

23.5 E-learning skills

E-Learning describes learning done with a computer which is usually connected to a network, giving users the opportunity to learn almost anytime, anywhere. Development of e-learning skills assures appropriate and effective application of e-learning to teaching and improves student learning. The E-learning unit shall develop training packages for both staff and students and put in place evaluation and support mechanisms to ensure quality assurance of materials. This unit shall also set up an e-learning laboratory to develop local capacity in development and evaluation of appropriate training software. Academic staff members shall continuously make use of e-learning to enhance the effectiveness of their teaching and provide students with an e-learning experience throughout their programmes of study.

24.0 ENFORCEMENT AND PENALTIES FOR VIOLATIONS

ICT systems depend on the collective effort and responsibility of all who participate in and manage their use. Any disruption, whether by technical or behavioral means, can impact on the availability, reliability and efficiency of the systems. Users are subject to the institution's policies and guidelines regarding the appropriate use of the shared resources. Any violation of the University Guidelines shall be considered a threat to the Institution's security and image shall be deemed as a serious offence.

24.1 Penalties

1. The ICT Centre shall suspend a user's access to its systems while the following are being investigated: Violations or suspected violations of security and/or policies

2. In the event of any investigation, the ICT board shall be

deemed to have given consent to system administrators to have access to a user's files as required to protect the integrity of the University ICT systems.

3. Workstation that may to be contributing to poor performance of ICT systems, including the network and Computer malfunctions may be disconnected

4. The institution's disciplinary committee shall handle all violations under this policy.

25.0 COMPUTER DISASTER RECOVERY

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives the University a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions but any event that could likely cause an extended delay or denial of service should be considered. There is the need for management to support ongoing disaster planning for the University. This policy applies to the management and technical staff of the University.

25.1 Contingency Plans

The following contingency plans followed:

1. Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?

2. Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.

3. Data Study: Detail the data stored on the systems, its criti-

cality, and its confidentiality.

4. Criticality of Service List: List all the services provided and their order of importance. It also explains the order of recovery in both short-term and long-term timeframes.

5. Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.

6. Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

7. Mass Media Management: Who is in charge of giving information to the mass media? Also provide some guidelines on what data is appropriate to be provided.

25.2 Action Plan

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster plan. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

25.3 Plans Update

Review all plans annually so that changes in the University's situation can be incorporated.

25.4 Enforcement

Any employee that violates this policy may be subject to disciplinary action up to and including termination of employment.