BOLGATANGA TECHNICAL UNIVERSITY

INFORMATION AND COMMUNICATION TECHNOLOGY RESOURCE AND SECURITY POLICY

OCTOBER, 2022

TABLE OF CONTENTS

1.0 Introduction

1.1 Purpose

This document outlines the Information and Communication Technology (ICT) Resource and Security Policy of Bolgatanga Technical University (BTU).

The policy is aimed at:

i. establishing the basic minimum infrastructure necessary for computerization and using this as a platform to shift the University's academic and administrative operations to a computerized environment through the implementation of the major corporate information systems (Library, Academic Management, Human Resource Management and Financial Management Systems);

ii. increasing the efficiency and ease of communication;

iii. enhancing learning and research through access to online resources;

iv. training user to ensure optimal utilization of the computerized environment;

v. equipping the ICT Directorate to ensure the availability of ICT resources through proper information resource management;

vi. modernizing teaching, learning and creating increased opportunity for access to quality and affordable education through E-learning;

vii. mitigating the risk of failure in a highly computerized environment through institutionalized data backup and disaster recovery;

viii. creating ease of access to all services by the University community while preventing unauthorized access and abuse.

Subject to approval by the academic board, this policy shall be publicized through the following channels:

i. Orientation programmes for new students and staff;

ii. ICT training of staff and students;

iii. BTU website;

iv. BTU staff and student mailing lists.

2.0 **Scope**

This ICT Resource and Security Policy is **NOT** a procedure manual for handling or using ICT systems or facilities. Procedure manuals shall be developed for specific ICT systems by the relevant IT support units for running and managing such systems. Procedure manuals are detailed guidelines that provide steps for handling the day-to-day operation and management of ICT systems.

This ICT Resource and Security Policy provides a framework for:

i. managing all ICT systems and electronic records owned by or licensed to BTU;

ii. secured and acceptable use of ICT facilities;

iii. managing the use of Internet and Emails;

iv. managing the University's website;

v. IT procurement;

vi. IT project management;

vii. individuals who are granted access to ICT resources and facilities owned and operated by BTU, including, but not

limited to, staff, students, researchers and visiting scholars.

3.0 ICT Governance and Service Management

ICT services in the University shall be managed by the:

i. ICT Directorate;

ii. Quality Assurance Directorate;

iii. ICT Committee.

4.0 Summary of ICT Services and Systems

ICT services and systems are designed to:

i. ensure availability of ICT services/systems at any workplace in the University and for selected services to locations outside the University through Common Network Services;

ii. ensure availability of User level Data Communication Services such as Email, Access to Internet/Intranet Services;

iii. promote Office Computing in all offices;

iv. improve both the efficiency and effectiveness of Library operations and services through the implementation of an integrated Online Library Management Information System (OLMIS);

v. enhance and streamline student education related administrative and managerial processes;

vi. improve academic reporting facilities at both central and Faculty levels through the development and implementation of an integrated Student Management Information System (SMIS);

vii. enhance and streamline financial management processes and reporting facilities at both central and faculty levels through the implementation of an integrated Financial Information System (FIS);

viii. enhance and streamline the Human Resource Management and administrative processes through the implementation of an integrated Human Resource Management Information System (HRMIS);

ix. promote the deployment of ICT in all areas of teaching, learning and research through creating technical and organizational preconditions;

x. ensure and require that all students, academic staff, managerial staff, administrative and support staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the ICT environment in their different functions;

xi. provide for the growth and financial sustainability of ICT resources through appropriate funding and operational mechanisms;

xii. leverage faculty/unit effectiveness and enable easier access to and coverage of the University education by using ICT in teaching, learning and research through the University wide implementation of E-learning;

xiii. ensure that ICT resources are secured and protected against abuse, damage, loss, harm or theft through the implementation of rigorous security protocols.

5.0 **Common Data Services and Office Automation**

5.1 ***Common Data Services***

Data Communication forms an essential component of the University ICT policy. It must ensure availability of ICT services/

systems at any workplace in the University. This Policy gives priority to the development and implementation of Data Communication Services at two different but related levels, namely:

i. Common Network Services - mainly comprising physical network infrastructure (wiring, switches, routers, servers, etc) and communication protocols (TCP/IP), are prerequisites for running systems such ARIS, OLIS and application-level communication services, such as email and Internet access.

ii. User level Data Communication Services - mainly email, access to Internet/Intranet Services, which actually are major "users" of the low-level network services.

5.2 *Electronic Mail Services*

Email systems are designed to enhance communication within the institution and with other institutions. An electronic mail system consists of the following components:

i. the user's frontend application, providing facilities for creating, addressing, sending, receiving and forwarding messages.

ii. the backend email server application that forwards messages from the sender to the receiver.

iii. a directory service, the Domain Name Service (DNS), that maintains a database with users and services on the network. Users access this service to locate the addressee and his or her email address.

5.3 *Access to Internet Services*

This 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.

5.4 *Internet/Intranet Services*

Intranet Services include facilities to design, develop and store information formatted as web pages and make them accessible through the LAN of the institution, while Internet services publish information on the World Wide Web. In general, both services use similar software and hardware technology.

Intranet Services may be used for online publication of parts of corporate databases, maintained by systems like SMIS, FMIS and HRMIS. Further, in an academic environment Intranet Services are applied to access course manuals and other study and research documentation.

6.0 **Monitoring and Control**

Internet is an unregulated medium, and thus susceptible to abuse. The Information and Communication Technology Directorate (ICTD) shall regularly inspect Internet files held on computers connected to the University's network, to ensure users have not accessed inappropriate sites or sites that have been expressly forbidden. To achieve this purpose:

i. inappropriate sites, such as materials relating to pornography, materials offensive on grounds including but not limited to ethnic origin, religion, politics and gender, will be filtered or blocked to ensure that users do not access them;

ii. any user who finds a possible abuse as well as security lapse on any system shall report the event to the ICTD;

iii. users who deliberately access inappropriate material or send inappropriate messages to others shall also have their Internet access withdrawn and shall be dealt with in accordance with the University's disciplinary procedures.

7.0 **Downloading**

The following shall be observed with regards to downloading content from online resources:

i. information that is downloaded from the Internet shall be used for official or academic purposes. Copyright laws shall be respected and the appropriate credit given to the author or the source of the information.

ii. the downloading of text or images which contain material of an offensive, indecent or obscene nature is prohibited.

iii. any software or files downloaded via the Internet onto the University's computers may be used only in ways that are consistent with their licenses or copyrights.

iv. no user may use the University's facilities knowingly to download or distribute illegal software or material.

v. no user may use the University's Internet services to deliberately propagate any virus.

8.0 **Penalty**

Any breach of these directives as outlined in paragraph 9.0 supra, may result in disciplinary action, including written warnings, withdrawal of access privileges to the Internet facility and suspension. Also, individual persons shall be held liable for any infringement of copyright laws as a result of downloaded information from the Internet or distribution of illegal software or materials.

The University also reserves the right to report any illegal activities to the appropriate authorities, *e.g.,* the Police for prosecution.

9.0 General User Administration System

In order to handle the large numbers at the University, there will be one user database, for the University common system. For students, as an example, names, addresses and departments/courses are collected for the purpose. The information on students is imported from SMIS while the information on employees is imported from HRMIS.

For the students, this means that the same account/email address and user ID can be used for the length of the program. The account automatically expires when the student is no longer active in SMIS. In the same way, expiry of employee accounts will be flagged by HRMIS.

9.1 *Office Computing Services*

It is the University's policy to promote Office Computing in all offices. In this context, the term, Office Computing refers to the application of ICT resources to support general office tasks. Major office computing applications include, word processing, electronic mail, spreadsheet processing, document storage and retrieval and desktop publishing.

It is the university policy to, as far as possible, use a combination of open-source and proprietary software in all office computing.

9.2 *Disclaimer of Liability for Use of the Internet*

The University is not responsible for material viewed or downloaded by users from the Internet.

i. Users are cautioned that some materials from the Internet could be offensive and inappropriate.

ii. In general, it is difficult to avoid contact with these undesirable materials while using the Internet. Users accessing the Internet

do so at their own risk.

iii. Users are to note that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is expected.

iv. Use of Peer-to-Peer (P2P) applications (e.g. bittorent) for file sharing and entertainment is deemed to be inappropriate use and is not permitted. P2P usage enables sharing and distribution of copyrighted works, and the Copyright law makes it illegal to make or distribute copyright materials without proper authorization from the copyright owner. The University shall enforce protocol or port level restrictions to prevent P2P activities.

v. Individual persons shall be held liable for any infringement of copyright laws as a result of sharing and distribution of copyrighted works without proper authorization.

10.0 End User Skills Development

It is the University Policy to ensure and require that all Students, academic and administrative staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the ICT environment in their different functions.

i. Student Computer Literacy

a. All Students in all Faculties are required to take the prescribed ICT introductory level module(s) that will be credit carrying modules within twelve months of first registration.

b. Teaching of Information Literacy to ensure lifelong learning.

ii. Staff Computer Literacy

a. Periodic computer literacy training/workshop

should be organized to meet the ICT skills needs of staff.

iii. Computer Facilities

a. Faculties, Schools and Centers should have the required computing facilities for Teaching and Learning at all levels.

b. Faculties, Schools, Institutes shall be required to incorporate a component in their budgets for ICT.

In line with the implementation of the different ICT services and systems, considerable knowledge and skills have to be developed among the end users so that they are able to:

i. use ICT services and systems effectively and as independently as possible.

ii. contribute to the specification, design and implementation of ICT applications.

iii. be aware of the shared responsibilities for equipment, software and data, and enforce an atmosphere of collective responsibility and system ownership.

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

v. establish and sustain effective, efficient application and data management and systems maintenance.

This Policy provides for the development and implementation of a consistent set of training programs with different levels for existing/potential ICT users: Students, teaching and research staff, clerical and secretarial staff, and general management staff.

Additionally, this Policy is to create organizational (trainer capacity,

training management) and technical (practice labs for students and staff; computer-based training tools, self-paced training mode; general access computer labs) conditions assuring continuous in-house ICT training capabilities, as well as sufficiency of access to computers for learning and research, in the long term.

The short and medium-term goals shall be aimed at creating, as rapidly as possible, a sizeable proportion of staff that is familiar with, and able to effectively use the ICT infrastructure in their daily work. At the end of the first phase of the training, the University expects that:

i. All students and staff at all levels are able to use standard application packages (word processors, spreadsheets, databases) as well as email and the Internet.

ii. Administrative chores like calling meetings and distribution of minutes and other documents are handle via email

iii. Students and staff interact more using online message boards, email, and online discussion forums. The traditional modes of interaction (notice boards, circulars) should be replaced for most activities.

11.0 Information Systems

11.1 *Library Management Information System*

This Policy seeks to improve both the efficiency and effectiveness of library operations and services through the implementation of an integrated Online Library Management Information System (OLMIS).

The Library Information System will integrate the following functionality:

i. Circulation Control System.

ii. Cataloguing Maintenance System giving a high quality of bibliographic records in conformity to the standard cataloguing codes practices.

iii. Online Public Access Catalogue (OPAC) to share resources among libraries in different locations.

iv. Acquisitions Control, including search of online sources of publications, online access to book dealers and book publishers and order placement, checking in, querying on order records.

v. Serials Ordering and Control.

vi. Statistical reporting and management information provision.

vii. Ability to subscribe or to access academic and scholarly databases online.

11.2 *University Management Information System*

University Management Information System (UMIS) comprises:

i. Academic Records Information System (ARIS).

ii. Financial Management Information System (FMIS).

iii. Human Resource Management Information System (HRMIS).

11.2.1 **Academic Records Information System (ARIS)**

ARIS is the generic term for the collection of ICT services designed to support student and education related administrative and managerial processes.

It is the University Policy to enhance and streamline student education related administrative and managerial processes and to

improve academic reporting facilities at both central and faculty levels through the implementation of an integrated Academic Records Information System (ARIS).

The ARIS will include the following functionality:

i. management of student personal records.

ii. admission of students.

iii. management of student academic performance records and student academic performance analysis.

iv. curricula and course records management (Academic Program Offerings).

v. class scheduling (time tabling).

vi. space and teaching staff requirements analysis.

vii. students' financial transaction management.

viii. online database query and reporting facilities.

ix. alumni records and activities.

11.2.2 **Financial Information System**

The financial management function in any organization encompasses a great number of closely related administrative and managerial processes.

It is the University Policy to enhance and streamline financial management processes and reporting facilities at both central and faculty level through the implementation of an integrated Financial Information System (FIS).

The following functionality is regarded as essential to the University financial management.

i. Budget preparation, implementation, monitoring, reporting and evaluation. Given the decentralized nature of budgetary management, it is the University policy to make these functions available to faculties.

ii. Debt management.

iii. Cash management.

iv. Foreign aid management.

v. Revenue management including assessment of financial needs, collection of gifts, determination of tuition fees, government appropriations, contracts and grants, investments, sales.

vi. Expenditure management including authorization of expenditures, personnel costs, vendors, awards.

vii. Personnel cost administration (payroll).

viii. General Ledger.

ix. Budget Ledger.

x. Commitment Ledger.

xi. Accounts Payable.

xii. Accounts receivable.

xiii. Fixed assets management.

xiv. Inventory Control.

xv. Cost accounting functions.

xvi. Financial analysis and Web technology based reporting capabilities.

11.2.3 Human Resource Management Information System

Human resource management refers to adequate utilization of human labour for productivity and attainment of the organizational mission, goals and objectives. In an institution of higher education human resources form a primary organizational resource, which is scarce, expensive and difficult to maintain.

It is the University Policy to enhance and streamline the human resource management and administrative processes through the implementation of a Human Resource Management Information System (HRMIS).

The essential functional requirements include:

i. establishing a human resource policy;

ii. planning short and long-term staff requirements;

iii. recruitment of staff;

iv. job evaluation;

v. appraisal;

vi. training of staff;

vii. salary administration;

viii. pension fund administration.

11.3 *High Level Reporting Applications*

The University will promote and support the development of high-level reporting applications that cut across all the corporate data bases using data mining and/or other approaches.

11.4 *Software Development*

The University seeks to develop internal capacity and to develop its own software for the major information systems in collaboration with other institutions and/or organizations.

11.5 *Access Rights*

The University will, 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 ensuring the integrity of such data and information and respecting the privacy of individuals.

12.0 Electronic Learning

12.1 *E-Learning*

It is the University Policy to leverage Faculty/Unit effectiveness and enable easier coverage and access to ICT in instruction, learning and research through the University-wide implementation of E-learning.

To support this policy, the University will:

i. create organizational and technical conditions to ensure continuous in-house e-learning training capabilities;

ii. ensure all students and academic staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the Digital Learning Environment (DLE) in their different disciplines.

iii. develop University wide and global e-learning networks based on academic interests' groups and research collaborations.

iv. establish the appropriate common DLE infrastructure and software responsive to academic needs through the designated central technological unit.

12.2 *E-learning Goals*

The following are the specific University goals and strategies that relate to the integration of ICTs in the teaching and learning processes.

Goal 1:

To improve the quality of graduates, by utilizing modern instructional materials and methods, including increased use of ICT in teaching and research.

Goal 2:

To provide greater access to University education, by developing capacity for increased enrolment through nonconventional approaches in teaching and learning i.e. Distance education and virtual University

12.3 *User Skills: Policy Drivers*

To achieve this policy objective:

i. students shall be required to take the prescribed introductory level module(s) as a requirement for e-learning;

ii. academic staff shall be required to demonstrate the prescribed level of competence for content development of e-learning within the DLE;

iii. new staff shall undergo training in education technology techniques with emphasis on e-learning;

iv. each unit shall set up an e-learning laboratory to develop local capacity in development and evaluating appropriate training

software;

v. units shall develop and nurture complimentary methods of teaching and learning, for e-learning as a medium of distance learning both within campus and outreach /upcountry centers, in the long term;

12.4 *Common DLE Infrastructure and Software*

It's the University policy to select the appropriate common DLE infrastructure and software responsive to academic needs through the designated management unit. To the extent possible, preference shall be given to open-source platforms.

12.5 *E-learning Management*

It is the University Policy to ensure sustainable management of the University's e-learning policy and resources through the creation of appropriate funding, advisory, management and operational organs that will cater for the broad interests of all users.

12.6 *Educational Technology Resource Function*

An Educational Technology Resource Function will be established, initially based within the Directorate for ICT Support (DICTS) but evolving to an independent Unit in the short to medium term, with the mandate of:

i. working as an E-learning Service function;

ii. coordinating e-learning activities;

iii. vetting proposals on e-learning;

iv. monitoring and evaluating e-learning;

v. promoting e-learning through awareness seminars, workshops etc.

The proposed unit will consist of people with ICT skills, teaching experience, technical, operational, and good communication skills.

12.7 *Faculty/Unit E-learning Team*

Within a Unit/Faculty an E-learning team will be formed. This will liaise with the central Resource Unit, to ensure implementation of agreed policies in the Faculty, and guide the development and implementation of faculty specific e-learning activities.

13.0 Data Communication Infrastructure

Data communication (DC) systems provide essential links between users of information and sources of information, and form the basis of the network infrastructure.

The policy is to develop a University-wide data communication network consisting of the following building blocks:

i. Inter campus WAN connections between campuses;

ii. Campus Area Network and

iii. Local Area Networks.

The University must set up a Data Centre (mail, web, administrative, library, etc.) specially designed with cooling, air filtering, UPS, backup facilities and physical protection, to ensure down-times are eliminated.

13.1 *Network Implementation*

A University-wide network infrastructure cannot be built overnight and will take a substantial period of time. For reasons of resource availability and management, the actual implementation will take place in a phased approach and will be synchronized with the implementation timing of different ICT services and systems as well as with the (expected/required) physical distribution of future

clients (users) and servers of each of the services and systems.

It is the University policy to design and implement all network segments under a single project management structure.

13.2 *User Security*

The University's ICT Security Policy is the collection of rules by which people who are given access to the University's information technology and data must abide. The main purpose of a security policy is to inform and guide users, staff, and managers of the requirements and their obligations in protecting technology and information assets.

The following are the basic requirements of securing network resources:

i. ensuring that only authorized individuals have access to information;

ii. preventing unauthorized creation, alteration, or destruction of data;

iii. ensuring that legitimate users are not denied access to information;

iv. ensuring that resources are used in legitimate ways.

An effective and feasible ICT security policy must demonstrate the following characteristics:

i. Confidentiality;

ii. Integrity and

iii. Availability.

The following measures shall be taken as part of ensuring security:

i. networks should be built entirely with standardized switches to eliminate the possibility of unauthorized access;

ii. all links between switches should be optical fiber and

iii. encrypted communication methods (like SSH instead of telnet, https ...) should be used by all University critical systems (e.g., financial, student databases and so on).

Security policy will be governed by a higher-level University Information Policy.

14.0 ICT Management

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 will 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.

14.1 *ICT Committee*

The ICT Committee will be responsible for:

i. monitoring and controlling the progress of all activities arising from the implementation of this Policy;

ii. monitoring and controlling the progress and the University's ICT operations;

iii. allocating resources according to the agreed master plan;

iv. budgeting for the cost of management, operations, maintenance, training and expansion through the University budget;

v. recommending proposals for cost recovery and cost sharing

and

vi. determining/approving ICT Policy adjustments arising from technology trends or new visions and strategies.

The ICT Committee shall be constituted as per the Statutes of the University.

14.2 *Directorate of ICT*

The Directorate of ICT shall be set up as provided for in the Statutes of the University. Sub-units shall be created to operate within the Directorate.

14.3 *General Information Resource Ownership*

14.3.1 **Ownership**

All ICT resources (computer, data communication device, software, network components, data storage) shall belong to the University. However, the ICT directorate shall be responsible for the management and monitoring of these resources and services.

14.4 *Hiring of External Expertise*

The University is allowed to hire certain support services from external venders only if it is cost effective and if the expertise involved is not available in the University. Outsourcing should only be done on the advice of and in consultation with the ICT directorate. External expert should work in the presence of an ICT staff.

14.5 *Student ICT Fees*

The University Management will put in place a technology fee payable by each student to ensure that ICT services and systems can be expanded and sustained at the level compatible with the University's needs.

15.0 ICT Security

It is the University policy to provide guidelines aimed at ensuring that ICT systems are protected from:

i. unfavorable environmental conditions;

ii. unauthorized access;

iii. malicious attacks (Virus, worms, Trojan horses etc.) and

iv. inappropriate handling by IT personnel and users.

This must be done by enforcing the use of the University's User Defined Policy, which covers:

15.1 *Hardware*

Hardware refers to computers and accessories, peripherals and networking equipment indicated as follows:

i. **Computers**: Servers, Desktop Computers, Portable Computers (Laptops, Notebooks), etc.;

ii. **Output, Input and Storage Equipmen**t: Disk storage systems, Printers, Photocopiers, Scanners, etc.;

iii. **Networking Equipment**: Routers, Switches, Modems, etc. and

iv. **Communication Systems**: VSAT (Very Small Aperture Terminal), Cabling Systems, etc.

15.2 *Hardware Environmental Conditions*

It is the University policy to provide guidelines aimed at ensuring that the environment within which the ICT systems operate are protected against power fluctuations, high temperature, high humidity, fire, dust, etc. This policy must ensure that, power

supply to computers and accessories must be stable, safe and uninterruptible. This will involve the provision of:

i. Stand-by generators/battery banks especially for centralized systems;

ii. UPS (Uninterruptible Power System);

iii. Stabilizers;

iv. Power protections devices against surges and lightning strikes

v. Smoke detectors and fire alarm systems at all Computer Labs and Server Rooms;

vi. Fire extinguisher(s) all Computer labs and server rooms. They should be periodically tested to ensure that they are in good working condition and

vii. adequate lighting system at Server Rooms and Computer Labs.

15.3 *Access Control*

The University access control policy ensures and defines guidelines aimed at:

i. preventing or minimizing unauthorized access to computer systems and

ii. preventing or minimizing damage, theft or loss of equipment.

The main levels of access control policy involve:

i. Physical Control

   a. The policy must ensure that Server Rooms and Labs are adequately secured.

   b. A logbook or electronic system must be maintained to

record entries and departures by IT personnel, visitors and service providers. Details of Date, Time, Personnel/ Student/Staff, purpose, and exit time shall be recorded in the logbook.

c. As part of the policy, provision (e.g., pigeon holes) should be made for safe keeping of student bags at the Computer Labs; bags must not be allowed into the labs and all students who use the labs must be duly authorized through a registration process.

d. It is the University policy to ensure proper asset management systems. User Departments shall track their computer systems through the use of an **Asset Register**. The Asset Register may be a notebook but preferably a spreadsheet with the following basic information: *Type of Equipment, Serial Number, Model, Specification, Date Purchased, Location (Room, Office), Cost, Life-Cycle (In Years)*, *and Status (in operation, faulty or under repairs)*.

e. The ICTD shall provide template for the Asset Register and make them available to user departments.

f. Asset identification: All IT Equipment shall be identified by an asset number. The asset number shall be engraved on the equipment casing.

g. Equipment Movement Tracking: An equipment movement log book shall be maintained to track movement of ICT equipment. Details should include equipment specifications, name of user, where the equipment is being moved from and to, why it is being moved and the date of removal and replacement.

h. Any IT equipment other than the individual's laptop taken off site must have the responsible Officer's authorization for removal.

i. Removal of any IT equipment other than laptops from its

normal place of use, e.g. from one lab to another for any reason, must be authorized by the responsible IT Officer and logged in the equipment movement log book.

j. Insurance: IT Equipment should be insured as part of assets insured by the University or Department.

k. Lost or Stolen Equipment: Lost or stolen ICT equipment must be reported to the Head of Department and the Chief Security Officer.

l. Security breaches must be reported to Head of Department and the Chief Security Officer. These include but are not limited to: unauthorized entry, doors left open or unlocked, faulty locks, broken window glass, windows left open, etc.

ii. Logical Control

The University policy on logical control in line with its user acceptance policy ensures that:

a. users of computing and networking facilities must be authorized through the assignment of User IDs and Passwords;

b. all guests and visitors to the University must sign-up for Guest User Accounts;

c. the essential 'dos and don'ts' shall be explained to such visitors and guests, prior to their use of the University's computer facilities;

d. users are advised not to disclose their personal passwords to anybody;

e. users are responsible for protecting their personal password and the consequences of their password being known by others;

f. users may not sign on to any University system using a user ID other than that assigned to them;

g. users are accountable for all system activities that occur using their user ID and password;

h. initially assigned passwords for any users must be changed upon first login and

i. good practice with passwords will largely be enforced by the system settings.

15.4 *Network Control*

The University's networking facilities are intended for teaching, learning, research and administrative support purposes. In view of this, this policy guidelines on network control access ensures that its network infrastructure is secured against:

i. Email Spam

ii. Intruder or Hacker Break-ins

iii. Malware

To avoid interoperability or poor network connectivity problems and in accordance with the University policy, User Departments are advised to contact the ICTD before installing or making any changes in their Local Area Networks (LANs) as well as workstations.

Users or User Departments shall seek clearance from the ICTD for any third-party network connections to the Internet or any external networks.

15.5 *Troubleshooting, Repairs and Maintenance*

To ensure sustainable repairs and maintenance of ICT equipment;

i. Desktop computers, Portables (Laptops, Notebooks, and PDAs) and Printers that develop faults should be sent to the ICTD for repairs and maintenance.

ii. IT personnel should document and keep system settings and drawings up to-date.

iii. the ICTD shall provide templates for maintenance contracts and make them available to user departments.

iv. user Departments shall liaise with the ICTD to arrange maintenance agreements with external ICT Service Providers.

16.0 Software

To safeguard and guarantee the safety of applications and systems, the following guidelines must be observed.

i. **Pirated** or **Unlicensed Software**: No pirated or unlicensed software shall be installed on individual workstations or on servers. The University should purchase her own corporate Software.

ii. **Copying of softwar**e: Users shall not allow the University's licensed software and/or associated documentations, to be copied by outsiders and may not themselves make copies other than those provided for in the relevant licensing agreements.

iii. **Faculty/Department software applications**: In order to benefit from volume discounts and common installation and setups, the ICTD shall coordinate the procurement and implementation of common software applications used by the academic units.

iv. **Software Configurations:** Software configurations should be documented for easier reference.

16.1 *Antivirus*

The University policy is to ensure that corporate standard antivirus Software is procured for the University use. The ICTD shall ensure that the relevant Antivirus is installed on all computers once notified. It is the responsibility of every user to avail their machines for the installation of the antivirus software. The Antivirus policy entails the following:

i. the ICTD will provide automatic updates of the antivirus through the network for computers connected to the network once a first-time installation is done;

ii. for computers not connected to the network, the officer in charge at the Department should liaise with the ICTD to have the updates done regularly;

iii. any software or data received from any external source, including the original manufacturer and from the Internet, must be treated as suspect and not be installed, executed or used in any other fashion until it has been scanned for viruses using the University's standard virus detection software and

iv. users should call the attention of the ICTD immediately for assistance if a virus incident or activity is noticed and cannot be cleaned by the user.

16.2 *Disaster Recovery*

Disaster recovery procedures and contingencies shall be defined and established for mission critical systems such as Internet, Email, MIS systems and Library Information Resources. The objective is to create capacity to restore services within acceptable period of time after a disaster such as major hardware or system failures or failures resulting from fire, flood and earthquakes.

17.0 ICT Procurement

The University policy provides the following guidelines for the procurement of IT hardware, software and networking products and services. When in doubt, user departments are to consult the ICTD for clarification or advice.

i. User departments must consult the ICTD before any contract with any ICT service provider is consummated;

ii. The ICTD will publish Contract Templates that may be adopted for ICT service contracts.

iii. **Warranty**: A minimum of one (1) year warranty should be specified for all technology acquisitions.

iv. **Desktop and Laptop Computers**: Computers purchased should have sufficient capacity to run applications at satisfactory response time for at least 5 years.

v. **Proven Technology**: Only proven hardware and software with available and very well-established support are to be acquired. Preference should be on proven technology.

vi. **Industry Standards based:** Technologies that conform to international industry standards shall be adopted. This will apply to hardware, networks, operating systems, databases and portable software. Proprietary technology and tools should be avoided where industry standard systems exist.

vii. **Compatibility**: New technology components should be compatible with one another and with the legacy ICT systems.

viii. **Upgradeability and Scalability**: Technology components acquired should be upgradeable and/or scalable.

ix. **Security:** The Technology component or system must have industry standard security in-built.

x. The ICTD should be consulted in the procurement of ICT equipment.

18.0 IT Project Management Guidelines

IT Projects are generally risky and shall, therefore, be managed using best Project Management practices.

Project Implementation Team

i. All IT Projects shall have a properly constituted Project Implementation Team (PIT).

ii. For a University-wide project, the PIT shall be constituted by the ICT Committee.

19.0 Sustainability

The University will develop a sustainable infrastructure (including information resources) with adequate provision of trained research support staff and relevant support services.

A key issue will be the provision of predictable and sustainable funding in the longer term to match future ICT developments and to enable effective development planning and progress.

The University policy will task the ICT Directorate to identify, promote and pursue strategic opportunities and alliances and engage with appropriate networks, projects and funding streams to support the development and sustainability of systems and services for learning and research

Five most common issues in connection with ICT sustainability include the following:

i. Funding: The University will adopt a variety of funding

mechanisms for the provision of ICT resources and services, and major development decisions can have unforeseen knock-on implications for ICT. Medium term predictability of funding is an important contributor to ICT sustainability. A clear ICT budget for infrastructural development must be defined;

ii. **Planning -** is a key contributor to a stable operating environment.

iii. **Management** – absolute support and management buy-in.

iv. **Staff availability and skills** – the recruitment and retention of requisite ICT staff.

To ensure that this policy is sustainable, the following measures should be pursued:

i. identifying sources of funding for acquisition and maintenance of equipment, and training ICT personnel;

ii. regularly updating of computers and related equipment according to their life cycle;

iii. networking to be a continuous process as new building facilities for academic and administrative purposes spring up;

iv. acquiring ICT hardware and software from a common source to reduce cost;

v. setting up a maintenance workshop and the use of ICT facilities to generate income and

vi. periodic training of ICT technical staff to up-grade their knowledge in modern trends.

20.0 Implementation

The ICT Resource and Security policy of the University aims at making ICT accessible.

The implementation plan of this policy takes into consideration the following:

i. the need for full stakeholder involvement and ownership;

ii. the need for competent human resource;

iii. recurrent and replacement costs and new acquisitions and

iv. acute funding gaps.

21.0 Policy Enforcement

i. The ICT Directorate in conjunction with the Audit Unit, and Planning and Quality Assurance Unit of the University shall audit compliance with this Policy from time to time. The outcome of the audit shall be a rating of the User Department compliance which will be published.

ii. The ICT Directorate shall be audited.

iii. Users who flout the policy provisions shall be sanctioned according to the regulations of the University or the sanctions specified in this Policy.

22.0 Sanctions

i. Any student, staff or employee who contravenes the rules and regulations, guidelines or procedures spelt out in this policy document shall be liable to sanctions.

ii. Appropriate sanctions shall be prescribed by the officer in charge or by a disciplinary committee constituted by the Vice Chancellor or his/her representative.

iii. For the avoidance of doubt, the appropriate sanctions shall include withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from

the University. The University also reserves the right to report any illegal activities to the appropriate legal authorities, *e.g.,* the Police, Copyright Administration Authority, National Communication Authority, National Information Technology Agency, *etc*.

23.0 Amendments to Policy

i. An amendment could be a modification of an existing policy guideline or an addition to the Policy.

ii. A member of the user community shall write to the ICT Directorate to propose an amendment to the Policy.

iii. The ICT Directorate shall in consultation with the ICT Committee study the proposal.

iv. If the proposed for amendment is found to be meritorious, it shall be forwarded to the Academic Board through the Vice Chancellor.