ICT POLICY Version 2

Approved by the Senate Executive Council on …/…../2016

UNIVERSITY OF TOURISM, TECHNOLOGY AND BUSINESS STUDIES (UTB)

P.O. Box 350, Kigali - Rwanda

Tel: +250-788 306692, +250-788306203

Email: info@utb.ac.rw /ict@utb.ac.rw

www.utb.ac.rw

DEFINITIONS AND TERMS

UTB: University of Tourism, Technology and Business Studies

ICT: Information Communication Technology

ICTU: Information Communication Technology Unit

IT: Information Technology

E- : Electronic

HOD: Head of Department

LAN: Local Area Network

ERP: Enterprise resource Planning

REVISION HISTORY

Date of Change	Responsible	Summary of Change
July 2014	ICT Policy Team	Updated and converted to new format.
July 2015	ICT Policy Team and External Organ	Updated and converted to new format.
July 2016	ICT Policy Team and External Organ	Updated and Adopted inclusion of Software System Infrastructure

Table of Contents

1. INTRODUCTION

In accordance with its broader strategic objectives, The University of Tourism, Technology and Business Studies, [hereinafter "the UTB University"] has procured and implemented at various locations, Information and Communication Technologies (ICTs) that are used to facilitate, promote, expend, create, process, store, share and disseminate data, services and information. These assets represent a significant economic investment by the UTB University. The data, Service and information resources they create, store and disseminate could well be priceless and irreplaceable. Their continued availability in furtherance of the UTB University's business is of paramount importance, hence, there is a compelling need to secure and control access to them.

Users of university electronic information systems and other stakeholders have an expectation of privacy for their personal data gathered by the UTB University in the normal course of its business. Therefore, there is a reasonable expectation from users that the UTB University would institute controls to conserve the privacy of personal information. Confidentiality of information is demanded by the common law, Rwanda national ICT Policy statute as well as Educational Institutions ordinances, regulations and convention. Since the UTB University operates on offering higher education services in a global marketplace, misuse of the institution's ICT assets and System infrastructure could degrade its goodwill and reputation.

The UTB University acknowledges that there is a well-founded requirement to maintain the integrity and confidentiality of its electronic data and information. Such assets must be protected from unauthorized access and intrusions, malicious misuse, inadvertent compromise and intentional damage or destruction. Accordingly, the UTB University is obliged to ensure that appropriate security measures are enacted for all electronic data, Services and information, as well as ICT equipment and processes in its domain of ownership and control.

This ICT policy has been developed for the general good of all users, and is aimed at ensuring that the University Information and Communication Technology (ICT) resources are utilized efficiently and for the sustainable benefit of all students and staff.

Information and Communication Technology (ICT) is provided to support the teaching, learning, research and administrative activities of the University. The data held on the network forms part of its critical assets and are subject to security breaches that may compromise confidential information and expose the University to losses and other legal risks.

This document constitutes policies and procedures for the management of all aspects of Information Communication Technology (ICT) services at the UTB with which all users (staff and students) must comply. Therefore any staff and/ or students using ICT resources is deemed to have made him/her self aware of these policies and procedures.

The effectiveness of this Policy and Procedures will be reviewed by the ICT staff and Management on a regular basis, and necessary amendments and additions made as and when required.

1.1 BACKGROUND INFORMATION

UTB MISSION AND VISION

VISION

To become a centre of excellence in the region for the quality of academic programs and to be a solution provider for the training of professionals in the area of Hospitality, Tourism and Business Information Technology.

Mission Statement of UTB

UTB is committed to spearhead the advancement of education though quality teaching, learning, research, consultancy and service to the community by preparing graduates to meet the needs of Rwanda, the sub-region and the global community.
UTB seeks to foster personal and professional growth in a conducive environment that values cultural diversity and cultivates the awareness of ethical issues, fairness, competitiveness and social responsibility.

UTB PLEDGES TO:

- Participate in the vision and aspirations of Rwanda by contributing to the development of the tourism industry through awareness raising of all Rwandans;
- Offer professional training to meet both local and international market demands;
- Improve the efficiency and effectiveness of both private and public tourism-related sectors through quality training, capacity building, research and consultancy services;
- Offer benchmarked programs to guarantee the competitiveness and employability of our graduates;
- Deliver academic awards of international standards through affiliated Colleges and Universities.
- Graduate students who are industry-ready.

1.2 UTB VALUES

RTUC seeks to foster personal and professional growth in a conducive environment that values cultural diversity and cultivates the awareness of ethical issues, fairness, competitiveness and social responsibility by:

- **Academic excellence:** The teaching, learning, and research of the Hospitality and Tourism sector shall from a core part of academic excellence at RTUC.
- **Culture of the University:** RTUC shall have a culture that values hard work, a culture that contends that hard work can lead to student success.
- **Equality of Access to Education and Training:** RTUC believes that all members of the community are entitled to equality of access to lifelong learning regardless of geographical location. The University College will therefore identify and use new and innovative learning methods to help ensure equality of access.
- **Equality and diversity:** RTUC through its policies shall embed good practice with regard to equality and diversity in all University college procedures and will also encourage the development of an inclusive curriculum
- **Quality:** The University is committed to continuous quality improvement and therefore recognizes that a strong focus on customer needs to be combined with self evaluation.
- **Best practices:** Institutional professionalism shall be reflected in our team spirit, exemplary ethos that reflect the highest standards, integrity, etiquette, honesty, and respect for every person.
- **Innovation and creativity:** RTUC shall work towards empowering its graduates to become job creators.
- **Environmental responsibility:** RTUC commits to respect and conserve the environment by adopting technologies that ensure efficient energy use, and waste management.

- **Engagement with society:** Promote Rwanda's social and economic advancement by responding to issues facing the society with a view to providing solutions to Rwanda scientific and technological problems.

- **Accountability:** RTUC shall be committed to openness and transparency and to gathering and seeking evidence from a variety of sources about its effectiveness in meeting its mission.

Non-compliance with Policy

Any concerned person who becomes aware of any violation or suspected non-compliance with the policies in this manual must immediately inform Management, who is responsible for taking any necessary corrective action after investigation.

Any possible non-compliance/violation needs to be reported in a written or electronic form in which the author of the report is identified. The person reporting the violation may request anonymity. Suspected violation must be communicated to the IT.

Policy Management and Update

a) A Custodian (IT) shall be formally designated for the update and maintenance of the IT policy manuals and their contents.
b) The Custodian shall be responsible and accountable for establishing and enforcing standard and consistent procedures to deal with any changes made to the existing IT policy.
c) The policy shall be systematically reviewed by the ITand any Head of Department at least once every 3 years and/or as and when there are IT or business related changes.
d) All changes to the manual shall be requested in an email to the custodian, including the following minimum details:
    i. Date of request
    ii. Originator of request
    iii. Policy or process name impacted, with corresponding reference
    iv. Description of change/update requested
    v. Rationale/benefit of the requested change

1.3 RESOLUTION OF THE POLICY

This ICT policy has been established to:

- ✓ Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources provided for use by academic, Administrative (Support) staff and students of the University in support of the mission and Vision of the University.

- ✓ Protect the privacy and integrity of data stored on the University network.
- ✓ Provide guidelines for the conditions of acceptance and obligations protecting Computer Lab Technicians and ICT Team Staff at large
- ✓ Mitigate the risks and losses from security threats to computer and network resources such as virus attacks and compromises of network systems.

- ✓ Reduce interruptions and ensure a high availability of an efficient network essential for sustaining the business of the University.
- ✓ Encourage users to understand their own responsibility for protecting the University network.

It covers the following security domains:

- ✓ The physical security of all computing and communication premises, computers, communication equipment and appliances, transmission paths and computer peripherals.
- ✓ The physical security of all storage media for data, system software, application software and documentation.
- ✓ The physical security of power systems supplying electrical power to network communication and computer systems.
- ✓ The logical security of data, information and information processing resources such as databases, MIS, Learning System, computer programs, email records, servers, routers, switches and other network appliances.

1.4 TARGETED AUDIENCE

These policy and regulations apply to:

- ✓ Users academic and administrative staff, students and others with access privileges using either personal or University provided equipments and E- Systems connected locally or remotely to the network of the University.

- ✓ All IT Equipments , devices and E- System locally or remotely connected to University network irrespective of ownership.
- ✓ ICT systems owned by the University and/or administered by the Information and Communication Office and/or other UTB Departments.
- ✓ All external entities or Personnel that have a contractual agreement with the University.

APPROPRIATE USE GUIDELINES

Do

- ✓ Use only those ICT facilities and services for which you have authorization.
- ✓ Use ICT facilities and services only for their intended purpose.
- ✓ Abide by applicable laws and University policies and respect the procedures.
- ✓ Respect the privacy and personal rights of others.
- ✓ Use University ICT facilities and services in a manner which is ethical, lawful and not to the detriment of others.
- ✓ Use University ICT facilities and services for teaching, learning and academic purposes.
- ✓ Use ICT facilities for personal use where such use is incidental and does not impose upon or adversely affect the University, such as using ICT facilities and services for occasional emails and web browsing.

DON'T

- ✓ Access, copy, alter or destroy information, electronic mail, data, programs, or other fi les without authorization.
- ✓ Use resources you have not been specifically authorised to use.

- ✓ Use someone else's username and password or share your username and password with someone else.
- ✓ Upload, download, distribute or possess pornography, pirated software, movies, or other unlicensed digital media.
- ✓ Send unsolicited emails (spam).
- ✓ Use electronic resources for harassment or stalking.
- ✓ Possess any "hacking tools" such as packet sniffers, password crackers, vulnerability scanners without written authorization from the Chief Information Officer (contact the Information Security team for assistance).
- ✓ Willfully waste resources associated with UTB's ICT facilities and services.

1.5 Roles and Responsibilities

ICTs are provided and deployed by the UWI to support the operational and administrative functions of Teaching, Learning, Research, and the management of its business. They are intended to be used primarily as business tools and to provide other support services.

General

The ICTs deployed are University facilities. All such technologies are and remain the property of the University , certain assigned Intellectual Property rights excepted.

Roles

Campus ICT Services Departments shall:

- ➢ Account for all ICTs and information resources in their area of jurisdiction that is connected to campus networks by one or other means.
- ➢ Provide and maintain a database of unique identifiers for all network-connected ICT assets.

- ➢ Assess the security risk of all ICT systems and apply such security systems and processes as are consistent with the mitigation of this risk.
- ➢ Provide and/or commission the physical security of all University servers, databases, backbone network switches and ICT management, teaching and learning platforms.

- ➢ Advise to Procure, implement and maintain the logical security systems as are necessary to

protect University electronic data and information assets from misuse, damage, loss or unauthorized access.

- Develop, document and publish the ICT security guidelines in accordance with and informed by best practice.

- Promote a security awareness campaign for users of University ICT systems and collaborate with functional departments to design and deliver end user ICT security awareness training.

1.6 POLICIES

Areas covered in this policy manual are:

PART 1:The use of Technology to enhance Teaching and Learning and Research at UTB

PART 2: The use of Technology to support IT management at UTB

2.1 IT Risk and Security Policy
2.2 Password Management Policy
2.3 IT Change Management Policy
2.4 Backup and Restore of Data
2.5 Virus Management Policy
2.6 Internet and E-mail Usage Policy
2.7 Wireless Policy
2.8 Mobile Handheld Device Security Policy
2.10 Configuration Management Policy
2.12 IT Asset Management Policy
2.13 Website and Social Media Policy
2.14 Data and Information Classification Policy

PART 1 THE USE OF INFORMATION COMMUNICATION TECHNOLOGY TO ENHANCE TEACHING AND LEARNING AND RESEARCH AT UTB

1.1 KEY DEFINITION

Blended learning: A mixing of different learning environments and approaches that often includes both face-to faceclassroom methods and computermediated activities in and/or outside the classroom.

Pure e-learning /Fully-online: Complete reliance on e-learning materials for use without any face-to-face classroommethods. The nuanced difference between pure e-learning and fully-online tends to refer to thedelivery platform. Fully online implies reliance on a web-based solution while pure e-learningis independent of the delivery platform.

Computer-assisted instruction: The use of instructional material presented by means of a computer or computer system to enhance instruction and facilitate interactive learning.

Digital library: An organized collection of electronic resources, including publications, webcasts, electronic books, etc., that can be accessed via computers on a Local Area Network (LAN) or a Wide Area Network (WAN).

Distance education / Distance learning / Distributed learning; A field of education that focuses on teaching methods and technology for students who are not physically present in a traditional educational setting such as a classroom.

Blended learning and pure e-learning can be thought of as examples of distance education. Distributed learning, although it tends to be used interchangeably, implies a more learner centered approach to the design of instruction

E-teaching: Involves the use of electronic instructional materials in both face-to-face and virtual classroom situations, and often nurtures interaction with information, materials, and ideas.

Internet-based learning / Web-based learning / Online learning / Virtual education: An educational approach that involves the use of the internet for delivering learning materials, and supports teaching and learning using various online resources. These terms tend to be used interchangeably among educators because of their reliance to an internet connection; however, they do refer to different technology approaches. For example, web-based learning relies on an internet connection and the use of a web-browser with appropriate plug-ins to run different applications while Internet-based applications require an internet connection but not a web-browser. The coredifferences among these terms are how theyare implemented from an InformationTechnology/Systems perspective.

Learning Management System / Course Management System: A web-based application for the administration, documentation, tracking, and reporting of educational programs. Other tools, such as digital libraries can be integrated as part of an LMS to make it a more robust learning environment.

Mobile learning An approach that involves the use of mobile technologies so that learners can access instructional materials remotely for just-in-time learning. This often entails the use of smart phones or tablets.

Video Teleconferencing (VTC): A way to engage people at different locations in synchronous interaction. VTC includes video and audio feeds streaming in real time. Virtual classrooms can be conducted using VTC tools that allow for live teacher instruction and feedback via audio/video interactions, whiteboard sharing, polling, breakout sessions

Massive Open Online Courses are courses designed for large numbers of participants, that can be accessed by anyone anywhere as long as they have an internet connection, are open to everyone without entry qualifications, and offer a full/complete course experience online for free (Openuped 2015).

Open access publishing usually refers to the worldwide electronic distribution of peer-reviewed journal literature in order to give free and unrestricted access to it.Open Content open content' and 'open courseware' are sometimes used to mean the wide range of resources to support learning and teaching

Open Educational Resourcesare teaching, learning and research materials in any medium, digital or otherwise, that reside in the public domain or have been released under an open license that permits no-cost access, use, adaptation and redistribution by others with no or limited restrictions. Open licensing is built within the existing framework of intellectual property rights as defined by relevant international conventions and respects the authorship of the work, according to the 2012 Paris OER Declaration (UNESCO, 2012, p.1)

Open and Distance Learning (ODL) - The terms open learning and distance education represent approaches that focus on opening access to education and training provision, freeing learners from the constraints of time and place, and offering flexible learning opportunities to individuals and groups of learners. Open and distance learning systems can usually be described as made up of a range of components such as: the mission or goal of a particular system, programmes and curricula, teaching/learning strategies and techniques, learning material and resources, communication and interaction, support and delivery systems, learners, tutors, staff and other experts, management, housing and equipment, and evaluation. (UNESCO, 2002).

Open and distance learning is a way of providing learning opportunities that is characterised by the separation of teacher and learner in time or place, or both time and

place; learning that is certified in some way by an institution or agency; the use of a variety of media, including print and electronic; two-way communications that allow learners and tutors to interact; the possibility of occasional face-to-face meetings; and a specialised division of labour in the production and delivery of courses (COL, 1999)

1.2.1 Background of the use IT in Rwanda

The *Vision for Rwanda*, adopted by the Government in 2002, sets out a vision, along with goal attainment strategies that are focused on the education and ICT facilitated human resource development for the country in the year 2020.

Naturally, the provision of education is a very expensive social undertaking. It requires many years of instruction to develop knowledgeable human capital. Recently In the education sector, instruction becomes even more expensive with the requirement of expensive equipment, physical facilities and highly educated lecturers.

1.2.2 Government Vision 2020

The Rwandan government Vision 2020 plan for Rwanda's social and economic development, ultimate goal is of being a prosperous nation by 2020, by cantering on a "knowledge-based economy."

Rwanda is progressing toward a smart country where the use of ICT in promoted in all aspects. Most of the services are now provided online using different devises to access services delivery. The banking system, revenues collection and all government services are being migrated towards online services so that services are being smarter and efficient.

1.2.3 Smart Education Rwanda

Within Smart Rwanda masters plan the government of Rwanda is looking towards smart education where education content will be given all Rwandans citizen within Higher learning institutions are requested to promote open educations that are not limited to classroom teaching methods, locations, or approaches to interactive learning through digitalized learning contents. It hopes to improve and transform educational environments by enhancing the learning opportunities via digital learning contents across the country

All higher learning institutions are requested to avail digital content to potential students and to increase the flexibility in teaching by promoting self directed learning approaches and bring education

opportunities for student regardless of where they are located by attracting more students and cost reduction without compromising the quality of education.

To align to the government mission and aspirations the UTB policy is to promote smart education in Rwanda by using information communication technologies.

1.3 E-learning at UTB

University of Tourism, Technology and Business Studies (UTB) offers e-learning classes in both credit and non-credit areas that require few (if any) on-campus meetings. Classes are designed to provide close interaction with instructors while also allowing greater time and space flexibility to serve the students' needs. Use of email, discussion boards, synchronous online chat rooms, Web conferencing, telephone, and face-to-face meetings occur to encourage effective communication with students and instructor or student-to-student interaction. These courses are rigorous and cover the same material as on-campus classes. Credits earned though e-learning course work are transferable and appear on transcripts just like any other class.

1.3.1 E-learning scope at UTB

The purpose of the E-learning System is to make knowledge and learning resources and some of the University programs available on-line and to build an e-learning platform for use in Teaching, Learning and Assessment. The following is the policy that will ensure that all staffs, Students (learners) and managers are empowered to use the e-learning system to its full potential and for the purposes for which it is intended, it will guide participants to join a UTB IVC (Internet Video Conference) event/Lectures and Study Materials from a computer rather than in a classroom.

1.3.2 E-Learning Goals:

- To provide an alternative education delivery system for greater access by our students;
- To provide flexibility of time and location;
- To promote the integration of technology in the learning environment;
- To promote globalization of education through electronic access to information and experts worldwide.

1.4 Purpose of this policy

The purpose of this policy is to promote smart education using innovative teaching methodology approaches at UTB

This policy will guide administrators, mangers, lecturers and students to transform the current teaching, learning practices towards maximize utilisation of the existing cutting edge technologies in teaching, learning and research.

This policy will support the following strategies

- To guide and provide direction for board of government of UTB and high administration to set priorities related to the content creation, students access and provide adequate support for both students and lecturers
- To ensure that Lecturers and students and using appropriate technogies to achive the UTB mission and objectives
- To facilitate the adoption of the effective use of information communication technologies for the purpose of teaching, learning and research.

1.4.1 Key Objectives to the Policy

The objectives of the E-learning Policy are:

- To have on-line learning resources made available to all students and staff.
- Make on-line learning the first option where appropriate to satisfy training requests that have been highlighted in Personal Performance Reviews (PPRs) and Higher Learning Instructions to involve ICT integrated in Teaching, Learning and Assessment.
- To promote and maintain the use of on-line learning by making it available for professionals and Students.
- Ensure that all learners have the required skills and further requirement to use the Online Learning System.
- To establish service area “Learning Leaders, employed students and Entrepreneurs” to support all learners in their workplace.

- To integrate the on-line resources to complement tutor led training and achieve a blended learning approach.
- Continually increase usage of on-line learning resources for new starters, induction, and continuous Teaching, Learning and Assessment performance improvement.
- To ensure that learners feel empowered to undertake on-line learning Studies as necessary and as if a Traditional class approach.
- The E-Learning policy and the Procedures that follows embody the following concepts:

1.4.2 To make e-learning available for both Degree Programs & professional courses.

People may get admitted to follow their studies and access work related e-learning programmes during work time and outside of working hours. This is intended to provide greater fulfilment of training needs, which will help to motivate Leaders/managers, employed students and Entrepreneurs. In this context Admission is self- decided to be on Campus studies and/or E-learning based studies. And the Study Materials soft and videos are set to be available to all students with respect the programs they have enrolled-in and their user authentications.

1.4.3 Who are UTB E-Learners students?

Students enrol in e-learning classes for the following reasons:

- All students (Full time, Part time, ...)
- No transportation
- Disability
- Work commitment requires extensive travel
- Personal commitment requires time flexibility
- Lack of child care
- Professionals/Managers/Leaders/Government officials/ Entrepreneurs and are not having enough time to come and attend in traditional approach except the time of Real Time Practical sessions

1.5 Guiding principles of Technology enhance teaching and learning at UTB

- Promote the use of 21 century skills in teaching and learning process
- Promote the independent learning culture
- Promote students cantered learning approaches
- Promote international collaboration with remote university worldwide which in line with UTB mission and vision
- Promote international Lecturers and students exchange program using information communication Technologies
- Promote active learning
- Avail program which are flexible, affordable which are not compromising the quality of the service
- Promote mobile learning where cutting edge and teaching resources will be available for students on different digital devices (laptop, smart phones,...) by using mobile applications for learning, communicating and research.
- Avail digital resources on multiple format for students access and usage
- Enhance teacher and students interaction using appropriate communication channels

1.6 Implementation strategies

a) The Faculty of Applied Sciences and Technology in collaboration with Deputy Vice Chancellor in charge of Academics and Research will provide direct supervision
b) The Directorate of Quality assurance will evaluate the quality of the resources provided for the students
c) The directorate of ICT will provide adequate ICT environment in terms of connectivity and ICT infrastructure and management
d) The Faculty of Applied Sciences and Technology will provide the training in terms of integration of ICT in teaching, Learning and assessment in collaboration with the office Deputy Vice Chancellor in Charge of Academics and Research
e) Selected key champions lecturers will support their respective department in terms of deployment (hours used in this activities will be counted within the workload of the champion lection)

f) The university will nominate a UTB innovative teaching and Learning and Research Committee
g) The university will nominate key lecturers champions to promote innovative teaching learning
h) The university will provide capacity building and technical support wherever it is required
i) Selected key champions lecturers will benefit additional training and academic incentives to promote usage and quality assurance and support peers.
j) Support students and innovative teaching and learning clubs
k) The university will enhance ICT infrastructure (internet, wireless and computer labs) on campus and avail online teaching, learning activities outside classroom
l) Students and Lecturers will be responsible for their own ICT infrastructure and connectivity outside classroom premises
m) UTB will promote students to own their own connecting devices (laptop, tablets)
n) UTB will collaborate via agreement with private companies to support students to get laptop loans and internet access on affordable prices.
o) UTB will collaborate with stakeholders to promote the use ICT in teaching and Learning

1.7 Curriculum Design

- Curriculum design should include the diversification of different teaching and learning approaches includes the use technology
- All curriculum of UTB will implement blended learning methods (Full time students and part time students will comply with HEC and UTB program requirement by focusing on innovative teaching methodology)
- Curriculum may vary in terms of flexibility and delivery methods

1.8 Development of learning materials:

- All teaching materials must be in electronic format (word, PowerPoint, Pdf, recorded video and produced and stored on knowledge management information of system)
- All produced materials under the contract with the university belong to the Lecturers and to the University
- Core reading resources and link and other teaching resources must be given to students where possible must be downloaded

- Study materials are being designed and reviewed by the module team via the leadership of the module leader
- The study material is developed by a team involving academics, curriculum and course designers, language specialists, tutors, relevant external stakeholders where possible. However, the curriculum design and development is predominantly done by academics and they are the co-owners of the content of the material
- All resources and activities to be given to students must be well prepared in advance andlinked with every session outcome.
- Open Education Resources (OER) can also be used to enhance the content of the study material.

1.9 Assessment

- Summative and formative assessment can be done online as well as offline
- Online assessment must be linked with sessions outcome and can be multiple questions as well file submission, plain text, chat, forum discussion, online class participation
- Online campus assessment should be invigilated and are encourage to ensure not examination malpractice
- Assessment strategies should includeboth summative (examinations) and formative assessment (Tutor Marked Assignments) used for making judgments about the achievement of the learning outcomes. Deciding on the assessment strategyis an essential part of providing evidence that the purpose and the intended outcome of the programme have been met. Where possible assessment will be submitted on digital systems

- Formative assessment include assignments, research project, group work project, portfolio of evidence, online participation contribute towards a final mark.

- Formative assessment should be integral to the development of the study material where students are encouraged to encouraged to engage with the content through a range of activities. Courses developers should alos provide feedback on the activities so that students experience a form of discussion that takes place in the classrooms.

- Timely feedback are required and must be uploaded on learning management information systems for evidence

- A databank of multi-questions will be created to promote students engagement for each modules.

1.10 Teaching and learning methods

- The teaching and learning methods used will be determined by the nature of the programme; the students' profile; and the students' access to resources
- The methods will include independent study of learning materials, completion of various activities, formative assessment tasks, tutorials, practical work and opportunities to interact with others as well as research activities.
- The methods will also include work-integrated learning as a planned component of a curriculum when outcomes can only be achieved through work-based experience.

1.11 Delivery channels

- Electronic Media : UTB encourage the use of electronic media in teaching and learning resources activities .

1.12 Technology -enhanced learning modes of delivery

Learning Management Systemall the content of UTB must be uploaded on online platform where teaching guides and resources will be shared with students.

mLearningor mobile learning is promoting Learning management information which are accessible on mobile devices and format which are appropriate for mobile devices.

Videoconference system: The use of Desktop videoconference systems and room based videoconference system can be used where the Lecturers or students are located in remote location

however in this case face to face are encouraged. The audio and image quality must be tested before the usage.

Digital library: an inventory of open access databases will selected and then posted on regular basis at UTB website of library page, Student and Lecturers must be trained on how to use them.

1.13 Lectures' Roles

- Prepare study material (Conceptualising and writing the study material)
- Prepare assessment (Set assignment questions and examinations)
- Train tutors, develop marking guides, moderate and also participate as a marker
- Facilitate teaching and learning processes
- Provide prompt feedback on students work and respond to queries timely.
- Conduct research
- Monitor the performance of students
- Attend and participate in professional development training sessions.
- Prepare adequate tutorial plans and give students academic advice.

The following resources must in place before the module start in soft copies before the module start

- Module guidelines,
- The modules will be divided into Sections according to Topics or weeks (According to Objectives)
- Each Topic will have:
- Objectives
- Indicatives content Outline (PowerPoint presentation)
- Resources Learning: (videos, links and core reading articles)
- Activities
- The content must be on learning management information system before the module start

Worksheet for Designing a Course - Fink (2003)

Module Name:_____

Learning goals for the Module:	Ways of assessing this kind of learning:	Actual teaching-learning activities:	Helpful resources: (e.g., people, things)
1.			
2.			
3.			

1.14 Learning management information system Help desk

- Learning management system administrator will provide help desk to Lecturers and students
- Faculty of Applied Sciences Technology will provide on job training for the entire academic staff
- Lecturers will train students on how to use the system
- All lecturers must be computer literate
- IT help desk be directed to the ICT Department (using email/phone) at **ict@utb.ac.rw** or call any ICT Officer for Physical support. The ICT staff will provide you with the answers to your inquiry within 30 minutes or less.

1.15 Standard related to the students

- All students must have access they own laptops and Mobile devises that meets University specifications to access the content of the learning management information systems
- All current registered students must be given online username and password to access their modules which they are studying.

- All students should visit regularly the content
- All students must be aware of all Digital resources at their own disposition
- All students must have credentials to access wireless, learning management information systems at campus
- Student should be responsible for their own wireless when they are located off campus
- A help desk for the students must be available and request must be handled within 48 hours

1.16 Student laptop policy

This section is in reference to the University Computer ownership Policy for all students, whether domestic or international.

- Where students of UTB are strongly encouraged to have a laptop computer and mobile devices .
- Student Owned Computing support team that's ready to help every student to get study materials, software for practical classes, soft-demos, access to E-library and WiFi.
- It is in this regards, University registrar remind all Business Information Technology, Computer Applications, Computing Information System, Computer Engineering, Travel and Tourism Management, Hotel Management, IATA UFTAA new and existing Students that they will be required to own a personal laptop computer that conforms to their studies, research in the respect to the current University minimum standards by the time they enter computer level courses and research works. This is a one machine per student requirement to facilitate Teaching and Learning Practice. University recommend new models are from Apple, Dell, HP, Positivo and Lenovo computers.
- For more information, Parent and guardians can contact ICT Unit or mail to ict@utb.ac.rw for additional information identifying the records sought.

1.17 RULES AND REGULATIONS FOR STUDENTS CONDUCT IN UTB COMPUTER LABORATORY

Purpose of this section

Computer laboratories are special places filled with lots of expensive and fragile equipment. In order for the ICT Department to maintain the equipment and an excellent learning environment we need to establish guidelines for behaviour in the Computer Laboratory.

These rules and regulations shall apply to all students. The term “Student” refers to a person who is enrolled for the time being at UTB.

- Ignorance of any regulation or any public notice shall not be accepted as an excuse for any breach of discipline. The UTB ICT laboratory timetable should be respected without any prior complaints
- The ICT laboratory will be open on hours provided in the ICT service guide
- To avoid inconveniences caused by outsiders or un authorized users of ICT laboratory, every student using the ICT LAB must possess the official UTB student ID card or any other authorized identification showing that he or she is a student of UTB.
- Because of limited number of computers available, no student is allowed to sit on a computer with Internet connection just browsing with internet and not on academic purpose for duration of more than 45 minutes per day, However Wi-Fi will be Opened to all student with their own Laptop/Handset.
- No student is allowed to operate, remove, take or displace any computer hardware, e.g. mouse, network cables, Power cable, key board, CPU, monitor, etc in the computer lab. Any student, who will be found in possession of the above computer accessories or replacing them from one place to another, will face disciplinary measures and lead to discontinuation from studies.
- Student in Workshop Computer Lab are allowed to disassemble /assemble computers with the assistance/control of Lecturer and/or Lab Technician
- Excessive downloading by students, introducing a virus onto the network, trying to hack into network are not allowed on UTB network.
- A student may not be allowed to enter into ICT laboratory at any time during academic year due to one or more of the following reasons:
- Any serious case of indiscipline.
- Grave violation of regulations governing UTB ICT Computer laboratory.
- Possession, stealing of computer accessories such as, mouse, key board, network cables, etc. or removing, displacing, taking, changing, and replacing computer accessories from one computer to another.
- Viewing pornographic pictures and movies in ICT Computer laboratory, unnecessary noise from music played from computer audios, this restriction or access lists should be done at the UTB server level.
- Possession of drink such as water, Fanta, Juice or food.

- Every student shall exercise the highest standard of caution in handling UTB property in computer laboratory to avoid any possible damages.
- Any student who willfully or negligently damages computer hardware (accessories) shall be guilty of an offence and this would lead to discontinuation from studies, in addition to other penalties, the student must pay a given fine to replace the damaged item .
- No computer laboratory property of any description shall be taken from its proper place without the written consent of the Director of ICT Department.
- Conduct which does or is likely to cause damage or violence to persons or property within computer laboratory would lead to discontinuation from studies.
- Using force or striking a fellow student, an ICT Staff, computer laboratory assistant or any other person at the University of Finance and Banking (UTB.) is totally prohibited.
- Unauthorized use or interference with any technical or other services or installation of computer hardware is not allowed in the computer lab without notification of ICT staff.
- Students should not open windows and doors open because this will prevent air conditioners to work effectively.

PART 2 THE USE OF TECHNOLOGY TO SUPPORT IT MANAGEMENT AT UTB

2.1 Need for IT Security Policy

IT is our support system and has become an integral part of our operations. As we further use IT as a mainstay towards achieving our goals, it is essential that the environment affected by IT remains totally under control. The IT Plan shall cover the entire range of IT operations, approach towards its use, control mechanisms and upgrade from time to time.

2.2 Policy Statements

Information Technology is the most effective tool to add value to our business process, face business challenges. The policy document will enable us to derive maximum benefits from technological innovations and facilitate continued adaptation and control of computer.

In order to fulfil one of our objectives of good lending practice, the IT Risk Policy is designed to manage and safeguard's critical information assets The Policy document provides a secure network that protects the integrity and confidentiality of information while providing a high quality. This Policy is framed taking into consideration the various security threats and also the security strategies to prevent (proactive strategy) and detect & react (Reactive Strategy) to ensure compliance with the local regulatory guidelines.

2.3 Personnel and Roles

Departments are responsible for protecting sensitive information and assets under their control according to the security policy and its operational standards. In case of interdepartmental activities requiring shared information systems, departments must jointly assess threats and risks, agree on security requirements, safeguards, terms and conditions and document them and submit them to be approved by the relevant committee.

2.4 Duties and Responsibilities of the IT Personnel

a) All aspects connected with Systems installations in , including computers, desktops, LAN, communication equipment, printer, etc.
b) LAN administration and maintenance
c) Implementation of computer systems for Business and other applications.
d) Installation of fixes, upgrades to software
e) Monitoring systems security obligations.
f) Annual Maintenance Contracts for hardware and software
g) Cataloguing of hardware/software
h) Maintenance of hardware/software breakdown logs
i) Planning and execution of upgrade of hardware/software
j) User trainings – In-house or external
k) Daily and periodical backups and archiving

2.5 Inventory of IT Infrastructure

To have a proper management of IT infrastructure available in , phase out obsolete infrastructure and ensure upgrade on time.

An inventory of IT infrastructure in has to be conducted and be updated accordingly and reviewed annually or as and when need is felt. Whenever any equipment is considered to be redundant / obsolete it would be replaced.

2.6 Physical Access

2.6.1 Physical SecurityAccess Control

Access to the system room where critical components like Server, Hub, UPS etc., would be **strictly** defined and restricted only to the IT Personnel and the top management. Entry by any other official or service/maintenance personnel would be allowed only in the presence of an authorized official. The event should be logged in the System Room access register kept for such purpose. Physical controls should not be dispensed with a case of officials visiting from Computer Audit agency or statutoryagencies. The officials would be allowed entry only after establishing their credentials and the need to enter the System room. The visit should be logged in the normal course. In case such officials

require access rights should be ascertained and created for the authorized purpose only. The rights would be revoked after the purpose is over.

2.6.2 Custodian of IT Related Keys

Custody of the keys of IT room and UPS room should be with the IT. The duplicate of all these keys would be in the custody of the Administration Department.

2.6.3 Hardware Security

Hardware security concerns safeguarding information technology equipment, the functions the equipment performs and the information that is processed, stored and transmitted by the equipment. Hardware security helps to ensure that information is not accidentally lost or altered within or between hardware devices. It also helps to ensure the availability of services that may be lost through the effects of interference due to electromagnetic emanations.

A common vulnerability in hardware security is inadequate policies and procedures for controlling changes to information technology systems, including those resulting from maintenance activities. This creates a significant security risk but the cost of minimizing the risk is low.

Departments must ensure that they have read, understood and implement the security policy and procedure for hardware security. In this policy, an attempt has been made to cover the following areas, but are not limited to:

a) Proper placement and installation of IT equipment to reduce the effects of interference due to electromagnetic emanations.
b) Maintenance of an inventory and configuration chart of hardware
c) Identification and use of security features implemented within hardware
d) Maintenance of information technology equipment and services.

2.6.4 Software Security

Software security concerns safeguarding applications, data, operating systems, programming languages, controllers and micro code embedded in devices that control some aspect of IT systems.

Software security encompasses administrative controls, quality assurance, development and maintenance procedures, management of the configuration, isolation and access, and audit controls.

2.6.5 Access to Business Critical systems

The University is dependent on several of its major systems for its daily operations. Breaches to their integrity, or their unavailability for any significant period of time, could reduce the service delivery capability or place the institution in disrepute. Such systems may include the Student Administration System, online teaching and learning platforms, the financial management system, the enterprise planning and/or human resource management information system. Notwithstanding the general security safeguards enunciated before, these business-critical systems shall be provided with an elevated level of security. These additional measures shall include, but are not limited to, internal firewalls, secondary access challenges and biometric access controls if any. When the security requirements are stringent enough, internal isolation of the network segment to which such systems are attached is the final consideration.

2.6.6 Privacy and Confidentiality

The University requires that the architecture, processes and procedures surrounding applications must be such that privacy of University data and information is protected. Users of University- supplied or supported applications must be advised of the procedures required to maintain privacy of University data and information.

2.6.7 Communications Security

Communications security concerns protecting information transmitted electronically, and guarding against the detection and interpretation of electromagnetic emanations from information technology equipment.

Unless protected, all electronic communications are vulnerable to such threats as hacking, interception and misdirection. Consequences of these threats being carried out include disruption in service, financial loss through theft of telecommunications services and unauthorized disclosure of information.

To safeguard security of information users need to ensure that appropriate steps are taken to ensure that personal data is protected from unauthorized access and disclosure, including limiting access to such data only to those employees with a business need to know.

2.6.8 Network Management

Departments should pay particular attention to reviewing the security requirements of local and wide area networks. There is a need to balance open information exchange with security to prevent unauthorized users from gaining access to sensitive information systems.

There are several types of network applications that want special attention from a security perspective, including electronic mail (e-mail) and electronic data interchange (EDI). Electronic data interchange is used widely in the financial field. The applications are often vulnerable to threats of fraudulent transmission, authorization repudiation and loss of data integrity.

2.6.9 Users' Responsibilities

The LAN/WLAN and the computers on the network are owned by the UTB and are intended to be used by staff to conduct work-related activities only, except personal laptops that are hooked up to the LAN to get Internet connectivity because they do not access it outside UTB. Reasonable care must be taken to ensure that no viruses are transmitted. The ICT Department will provide guidelines and practical hints to all users on how to protect their computers. Anyone found misusing the UTB computing facilities will be dealt with through disciplinary processes and procedures.

The following, among others, are deemed to be Inappropriate Usage of network resources:

- Using the computing systems to conduct ones personal business.
- Installation of any software on the LAN computers without first officially clearing it with someone in the ICT Department. This includes any software downloaded from the Internet as well as any personal software from other sources.
- Installing any unauthorized software can in turn create problems with the functioning of our computers and/or the software installed on it.
- The downloading or electronic distribution, displaying, or printing of any material that may be deemed offensive by anyone (including pornography) is also deemed highly inappropriate.

The ICT Department has the sole authority to install, upgrade, delete or maintain any hardware, software or any ICT equipment on the network.
Any staff found breaching this policy without the approval of the Director of the ICT Department will have his/her access to the UTB network suspended, and disciplinary action instituted.

2.6.10 Access to UTB ICT Infrastructure facilities

Access to UTB computer facilities is limited to only UTB staff and currently enrolled students. Exceptions are made for UTB academic pursuits, and approved workshops, seminars, or other special events. Users are responsible for ethical use of UTB computer resources, including both honesty in their academic pursuits, and respect for others who share these resources.
If requested, users should be prepared to sign in, and/or may be requested to present a valid staff/student identity card when found using UTB computing facility.

Respect for other users

When using the facilities in the computer Labs, there should be silence and respect for other users. Loud conversation and disruptive behavior will not be tolerated, and such users may be requested to leave the facility, and further action may result in one being banned from using the Labs.
Users may not encroach on others' use of computing resources. Such activities include, but are not limited to, sending harassing messages, introducing viruses or anything else which damages software or hardware, and misrepresenting one's identity in electronic communication.

2.3.11 Reducing wasteful use of paper and printing Supplies

Users are expected to be conservative in their use of printing paper, and to exercise discretion when printing documents, to prevent waste of expensive printing materials. Because color cartridges are costly, users must be prudent when sending print jobs to color printers.

Users are expected to exercise good judgment when submitting printing tasks and take proper care of the computers, printers and all other equipment found in the facilities.

Users should submit the print command only once to avoid printing multiple copies of a document.

Users should allow adequate time to ensure a successful execution of a print job before re-sending a print command. Users who need multiple copies of a document must use a photocopying machine for duplication of documents.

Users are urged to use the “print preview” command before submitting a print job. Blank pages that appear in the “print preview” result should be deleted before the print job is sent. Users should make sure they have sent their printing job to the correct printer. To do this, instead of immediately clicking on the printer icon, users should click the File command in the main menu toolbar, and then select “Print,” which will open the Print dialog box where settings can be checked and adjusted before sending a print command. Users must only print materials of academic relevance or curricular significance.

Users should notify the ICT staff if the printer has failed to respond correctly after the first print command. If users have submitted an incorrect print job, they should notify the ICT staff so that the staff can attempt to cancel the job or you may do it yourself, if possible.

2.6.12 Computer account and password guidelines

Information stored on the computer desktop, laptop and the LAN (Local Area Network) forms a part of the University's valuable assets. A user can gain access to all network resources with the use of a single username and password.

Passwords are an important aspect of computer security. A poorly chosen password may result in guessable password giving unauthorized access and/or exploitation of UTB's resources.

All users, including contractors with access to UTB systems, are responsible for ensuring ensure that only authorised individuals have access to specific computer systems and establish accountability for all changes made to system resources. Strong passwords promote a secure computing environment; badly chosen passwords endanger the information that they are supposed to protect.

Creation of strong protection password standards, their frequency of change is outlined below.

✓ Users must guard against responding to emails asking them to provide their username and password for system maintenance, even if the email appears to originate from UTB mailing system. These emails are fictitious and are an attempt to steal a user's identity for nefarious purposes.

✓ Passwords must be kept confidential and not shared with colleagues. This does not apply to unit and departmental passwords, where a group manages the password and in such cases, the password must not be shared outside the group.

✓ Passwords must not be based on personal information (e.g. names of families, birthdays and other personal information such as addresses and phone numbers)

✓ Passwords must not be revealed to anyone over the phone even if the recipient is a member of UTB staff.

The password must not be a word found in a dictionary in any language

All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. All users at UTB should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

Contain at least three of the five following character classes:

- Lower case characters
- Upper case characters

- Numbers
- Punctuation
- “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least fifteen alphanumeric characters.

If an account or password compromise is suspected, report the incident to the ICT Department

2.6.13 Monitoring Electronic Mail (E-Mail), Internet and Intranet, Website

Sending messages by e-mail is so convenient that unprotected sensitive information is often transmitted this way. Without protection, the confidentiality of e-mail traffic can be compromised by radio intercept, casual eavesdropping at message storage points or by deliberate monitoring of the circuit. The integrity of e-mail services can be compromised by poor design of the information system. A key integrity concern is the possibility of an e-mail message never reaching its intended recipient and the sender being unaware of that fact.

2.6.14 Email and Electronic communication

E-mail has been established as a major communication tool within and outside the university .the ICT Department wishes to encourage the correct and proper use of e-mail, and expects staff to use this facility professionally and ethically during their normal course of work.

All staff is obliged to communicate using UTB official email addresses UTB webmail and Outlook facilities are operational.

a) Email is a business communication tool and users must use this tool in a responsible, effective and lawful manner.
b) Users shall avoid opening mail from unknown users/sources and also avoid opening suspicious attachments or clicking on suspicious links.
c) shall restrict attachments size on the company mail system.
d) reserves the right to monitor email messages and may intercept or disclose or assist in intercepting or disclosing Email communications to ensure that email usage is as per this policy.
e) Users shall avoid any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

f) Users shall avoid unauthorized use, or forging, of email header information.

Email access is available to all staff and Wi-Fi is Open to all students that are registered at UTB.
Request for new recruited email accounts creation should be addressed to the Director of ICT in electronic form by the Director of Administration and Human Resources Management whom also must inform the ICT Department any staff resignation cases for staff account termination.

2.7 Email Policy

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.
The purpose of this email policy is to ensure the proper use of UTB email system and make users aware of what UTB deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within UTB Network.

Scope

This policy covers appropriate use of any email sent from UTB email address and applies to all employees, senor managers, and promoters operating on behalf of UTB and must be in compliance with UTB core values.

Policy:

1. All use of email must be consistent with UTB policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

2. UTB email account should be used primarily for business related purposes; personal communication is permitted on a limited basis, but non- related commercial uses are prohibited.

3. For the purpose of uniformity the UTB webmail user e-mail address must be of their positions and the e-e-mail signature my contain full name of staff, department he has been appointed for and University address information.

4. All data contained within an email message or an attachment must be secured according to the Data Protection Standard.

5. Email should be retained only if it qualifies as a University business record. Email is a University business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

6. Email that is identified as a University business record shall be retained according to University Record Retention Schedule.

7. The University email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any University employee should report the matter to their supervisor immediately.

8. Users are prohibited from automatically forwarding University email to a third party email system. Individual messages which are forwarded by the user must not contain University confidential or above information.

9. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct University business, to create or memorialize any binding transactions, or to store or retain email on behalf of University. Such communications and transactions should be conducted through proper channels using University approved documentation.

10. Using a reasonable amount of University resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a University email account is prohibited.

11. University employees shall have no expectation of privacy in anything they store, send or receive on the University's email system.

12. University may monitor messages without prior notice. University is not obliged to monitor email messages.

13. (SPAM) AND PHISHING It is important that you do not respond to, or click on, any links in spam, phishing or suspicious emails, in particular emails that ask you to provide your username and password details, or any personal information. Phishing emails often try to create a sense of urgency by stating such things as:

- ✓ ‘Your account will be closed down unless you log on’
- ✓ ‘A recent security upgrade means that you have to log on to be protected’, or

‘There has been a problem with processing your payroll; you need to provide your account details to confirm that they are correct.’ If you receive a spam or phishing emails please forward the email to ict@utb.ac.rw and promptly delete the email.

Leave,Vacation,Travel, Desertion

Inordertoensurethatofficialinformationheldinastaff’smailboxisavailable whenstafftakesleave, vacation or travels, thefollowingmeasures shall betaken:

1. For staff about to take leave,vacationor travel, theEmail shall be set to automatically inform sender soft he ir *out-of-officestatus*, with an advice to send the message to an alternative Email address if itis official.
2. Staf fravelling outside or within the country, have the option of setting the Email to forward mail messages to analternative Email system where it would be easier to retrieve.
3. Staff deserted or resigned, HR have the option o request for setting inactive the Email or automatically change the password.

Usage UTB Mailing system (allstaff@utb.ac.rw)

The allstaff@utb.ac.rw mailing list is available on the university's website to facilitate easy communication at the university. This facility must be used to send messages frequently to a large number of people for things such as newsletters, announcements, decisions taken in management meeting and other helpful information that need to be disseminated to staff, none is allowed to use it amusingly like religious reflection, the mailing list will be updated on monthly basis .

Outlook mailbox keeping

The amount of e-mail in the personal Inbox should be kept to a minimum and the inbox should not be used as a storage facility. Unless required for audit purposes, e-mails should be deleted after reading, response or action.

The email system is designed for the transmission of messages and is not designed to be an archival system; staff should not rely on the email system as a safe archive for important documents. E-mails should be reviewed on a monthly basis and deleted when no longer required. The same housekeeping rules apply to Sent Items.

The deleted items folder should be set to clear all deleted items upon exiting outlook. Any e-mails that need to be saved should be moved to a personal folder (PST file). PST files should always be stored on a network drive to ensure they are backed up to prevent any data loss or corruption.

Out of Office message

UTB staff who will be out of the office for specific period must inform the UTB community and partners that he/she is out of office .staff should ensure that their out of office message includes details of when they will be back in the office, who should be contacted in their absence and include e-mail addresses and /or telephone numbers.

2.8 WEBSITE AND SOCIAL MEDIA POLICY

2.8.1 Website Governance

1. Website Manager (Webmaster): There shall be a Website Manager (Webmaster) who will provide quality assurance on the Content, Look and Feel of the University's Website ensuring that it is in tune with the University's mission, unique identity, ore values and status.

2. The Webmaster shall be responsible for setting policies governing the nature, content, format, maintenance, timeliness and ownership of information contained on the official pages of the website.

3. Public Relations Unit (PRU): The Public Relations Unit (PRU) shall be responsible for maintaining the content of the Home and main web pages. Information to be put up on these main pages shall be routed through the PRU. The PRU shall then proof read and edit the content. It will have an officer designated as a Web Assistant. The Web Assistant shall be responsible for updating the website and responding to Emails.

4. ICT Unit: The ICT Unit shall provide technical and advisory support services for the website. The ICTU shall be responsible for maintaining the University's web server.

2.8.2 GENERAL GUIDELINES FOR WEB PAGES

The following guidelines apply to all web pages of the University Website under the control of the University:

1. Content Management System: All web pages or websites shall have a Content Management System (CMS) that provides the capability for a Marketing Officer who has no web programming skills to update the information on the website.

2. Identification: All web pages shall be identified by the University logo or logotype.

3. Contact Information: All web pages shall carry the Email address of the department or officer in charge for their upkeep. The Administrative Assistant to the Central Secretariat shall check for info@utb.ac.rw Email and respond or forward.

4. Legal Compliance: All pages may not violate the University's policy and Statutes, copyright, libel, obscenity or other local or national laws.

5. Commercialization: Web pages may not be used for commercial purposes, sales or money-making ventures except those authorised by the University administration.

6. Accuracy and Currency: All pages shall be accurate, well-written, concise, and free of spelling and grammatical errors, and shall otherwise present the University's mission and values in a positive light.

7. Monitoring: All pages shall be regularly monitored by the Web Master in collaboration of Marketing Director to ascertain that material is current or appropriate. Outdated or inappropriate materials shall be removed within five working days when they are noticed.

8. Enforcement of Website Policy:

a. Any staff, student or individual that notices an error or considers content on the website to be inappropriate may bring it to the attention of the Public Relation Officer (PRO) and Marketing Director in charge.

b. The PRO or Web Assistant shall take measures to address the concern and give a feedback to the complainant.

c. The following shall govern the escalation procedures if the issue has far-reaching implications:

i. Head/Secretary/Web Assistant of a department shall escalate to Public Relation(PR) and Marketing Officer.

ii. P R O escalates to Webmaster.

iii. Webmaster escalates to Head of ICTU.

iv. Head of ICTU escalates to ICT Management Committee.

d. Where an individual who reported a problem on the site is not satisfied, the complaint may be escalated to the Academic Board.

e. Any page on the University site that violates policy may be removed from the website immediately by the Web Assistant of the Department or PRU or the University Webmaster.

2.8.3 Website Structure and Content

The website shall be made up of the following web pages:

1. Main University Web Pages: These shall comprise the University Home Page and pages that provide:

a. The profile of the University, *ie*, the governance structure, the courses and programmes of the Schools, Faculties, Institutes and Centres, as well as the administrative departments.

b. Admission and registration processes and requirements.

c. University Policies and Regulations.

d. News, events and announcements.

2. Departmental Web Pages: These shall comprise the pages or website of the respective Schools, Faculties, Institutes and Centres of the University. These pages shall provide details of the courses, programmes as well as academic staff. Personal web pages of Staff may be set up under the Departmental websites.

3. Student Web Portal: This shall be made up of pages that capture the life, programmes and activities of students.

4. Affiliates Websites: These are the websites of the affiliates of the University that University may choose at its own discretion to have links.

5. Others Website: These are sites that the University may have links to, for the purpose of collaboration.

2.8.4 Website Rules and Regulation

7.4.1 M a i n University Web Pages

1. The Public Relations Unit shall be responsible for updating and maintaining the content of the main University web pages.

2. The content of the main University web pages shall reside on the University web server.

2.8.5 Departmental Web Pages

1. By default, where a Department does not have a website, a minimum number of web pages on the University web server shall be allocated to publish information about the Department.

2. The PRU in conjunction with the ICTU shall create a standard set of pages for Department. However, responsibility for maintaining information on the website shall rest with the Department's Web Assistant.

3. Departments may choose to have a website of their own which may be hosted outside the University's web server. In this case a link will be established on the University's website to the Department's site. Based on the policy provisions in this document, the PRU in consultation with the ICTU shall approve of the establishment of links to departments that have established their own websites.

4. The web pages of Department-owned websites shall comply with the policy provisions in this document. Websites that do not comply may have their links removed. The decision shall be made by the Webmaster. This regulation applies to personal pages of Faculties.

5. The PRU shall ensure that information on all Departments, *ie*, Schools, Faculties, Departments, Institutes or Centres is available on the website.

2. 9 Social Media Policy

Introduction

This policy provides guidance for employees and Students use of social media, which should be broadly understood for purposes of this policy to include blogs, Facebook, whatsapp, Twitter, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit University Users to share information with others in a contemporaneous manner and marketing.

Social Media Policy

2.9.1 Objective

This policy will guide employees about the correct use of social media, which should be thoroughly understood. For the purpose of this policy the followings are included: blogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites and services that enable users to share information with others in a synchronous manner.

This policy outlines the standards that employees are required to observe when using social media, the situations during which the employee's use of social media will be monitored and the actions which will be taken in respect of breaches of this policy.

2.9.2 The Importance of IT Policy for Social Media

The use of social media is very important for as it can bring significant benefits in terms of building strong relationships with its current or potential clients. In order for this policy to work effectively, 's employees need to follow the rules and regulations correctly so as to increase the 's prospects.

's reputation can be damaged if employees breach the rules and make serious mistakes such as a misjudged status update. As a result, there are security and data protection issues to consider.

This policy describes how the 's employees can use the social media effectively and securely.

2.9.3 The Purpose of Social Media Accounts

There are different purposes which are associated with a 's social media accounts. The use of social media accounts should always be in line with the 's objectives, that is, an employee can only be able to post updates, messages and use the accounts after full consideration of the 's objectives.

An employee can make use of the 's social media accounts only to:

a) Respond to Customer Enquiries and help requests
b) Share blog posts, articles and other content which is generated by
c) Share content such as articles, videos, media and others which are relevant to the
d) Give the 's followers a vision about the inside of the
e) Support marketing campaigns and other offers
f) Encourage and stand up for new products which are launched and other initiatives

2.9.4 Scope

This policy applies to all staff and non-staff at who use social media while working – no matter whether for business or personal reasons. The social media use can be either on premises or while travelling for business or while working at home.

The use of the Internet at the UTB is a privilege offered to staff, students and authorized guests. The use of the Internet (LAN and Wi-Fi) is intended to be a research/learning tool for official purposes e.g. project research, reports, presentations, etc.
Users are not allowed to view any web sites that may have the potential of offending any fellow staff (i.e. pornography, hate sites, gambling sites, or any web site whose purpose is to willfully commit illegal acts or sell illegal material).

These are some social media sites and services which are involved (but are not limited to):

a) Popular social networks such as **Facebook** and **Twitter**
b) Online review websites such as **Reevoo** and **Trustpilot**
c) Sharing and discussion sites such as **DelilTus** and **Reddit**
d) Photographic social media websites such as **Flickr** and **Instagram**
e) Question and answer social websites such as **Quora** and **YahooAnswers**
f) Professional social networks such as **LinkedIn** and **Sunzu**

2.9.5 PROCEDURES

The following principles apply to professional use of social media on behalf of UTB University as well as personal use of social media when referencing UTB University.
• Employees need to know and adhere to the UTB University's Code of Conduct, Employee Handbook, and other company policies] when using social media in reference to UTB University.
• Employees should be aware of the effect their actions may have on their images, as well as UTB University's image. The information that employees post or publish may be public information for a long time.

- Employees or Students should be aware that UTB University may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to UTB University, its employees, or customers.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.
- Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized UTB University spokespersons.
- If employees find encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with employee's responsibilities at UTB University. UTB University's computer systems are to be used for business purposes only. When using UTB University's computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, UTB University blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Subject to applicable law, after-hours online activity that violates [the Company's Code of Conduct] or any other company policy may subject an employee to disciplinary action or termination.
- If employees publish content after-hours that involves work or subjects associated with UTB University, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent UTB University's positions, strategies or opinions."
- It is highly recommended that employees keep UTB University related social media accounts separate from personal accounts, if practical.

2.10 Password Management Policy

Objective

The purpose of this policy is to minimize the risk of unauthorised access to information resources by providing greater assurance of user authenticity through effective use and choice of passwords.

Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services.

Scope

This policy applies to

- All use of passwords
- Allemployees who use passwords as a means of accessing the data processing environment of .

Policy Statement

Password is the most common method for users to authenticate themselves when entering computer systems or websites. It acts as the first line of defence against unauthorised access, and it is therefore critical to maintain the effectiveness of this line of defence by rigorously practising a good password management policy. This policy aims to provide a set of guidelines and best practices for handling and managing passwords.

Threats and Risks

One of the most vulnerable parts of any computer system is the password. Any computer system no matter how secure it is from network or dial-up attack, viruses, and so on, can be fully exploited by an intruder if he or she can gain access via a poorly chosen or poorly protected password.

Password Change

Password should be changed within a short period of time and new password would be created.

Suspected disclosure forces password changes

Passwords must be changed as soon as possible for users who report that their accounts may have been compromised.

Enforce strong passwords

Many systems and applications include functionality that prevents a user from setting a password that does not meet certain criteria. Functionality such as this should be leveraged to ensure only Strong Passwords are being set.

Periodically Change of Password

Users must be forced to change their passwords periodically. As a general rule of thumb, changing your password every 60 days is recommended. However, you may choose to vary the frequency of password changes based on the privilege or access level of the account. Accounts of greater privilege or access level should have their password changed more frequently and vice versa.

2. 11 IT Change Management Policy

Objective

To ensure that changes to the IT infrastructure, applications, databases and reports are made in a consistent, systematic and controlled environment to streamline processes and mitigate security vulnerabilities and potential loss due to system outages.

Scope

This policy applies to all changes made to the following:

a) IT infrastructure including operating systems, computer hardware, networks
b) IT systems (refer to section 2.4Backup and Restore Data Policy for the list of IT systems)
c) Databases
d) Reports within any IT system

A change is any modification to hardware or software that has the potential to interrupt service, alter functionality or provide new technology ability.

Changes not covered by this policy are those that affect only an individual. Examples of changes not covered under the scope of this policy include, but are not limited to changes to an employee's desktop or laptop computer, allocation of IP addresses to a user workstation, updates to an office phone. Such changes shall be made following the IT Incident and Problem Management procedure.

2.12 Requests for Changes

All requests for changes shall be made in writing using the Change Request Form (CRF) to the IT.All change requests received by ITshall be centrally logged in the Change Request Log. The log shall contain at least the following:

a) Date of request
b) Date of change
c) Owner and contact information
d) Nature of change
e) Purpose of change
f) Indication of success, failure or work in progress

2.12.2 Authorisation of Changes

Users must obtained prior authorisation of all changes from their head of Department. All requests for changes shall be formally presented to the ITwho will obtain approval and authorisation in accordance with this policy.

2. 13. Backup and Restore of Data Policy

Objective

To ensure that applications and data supporting the operations of canbe completely and accurately recovered within reasonable timeframes in the event of a system failure, intentional destruction of data or disaster.

Backup Strategy Formulation

The ITshall be responsible for validating, documenting and maintaining the backup strategy covering all IT systems. Data locations (files/folders) to be backed-up on each IT system shall be formally documented and approved in the Backup Strategy.

2.13.1 Responsibility for Backup

Each System Owner shall be responsible for ensuring that backup is performed in line with the documented Backup Strategy.

2. 13.2 Execution of BackupProcedures

All data shall be backed-up by IT staff/System Owners in compliance with guidelines documented in the Backup Strategy

2. 13.3 Storage of Backup

All media on which data is backed-up shall be kept in secure onsite and offsite locations accessible to authorised personnel only. Details of the movement of backup media shall be documented in a Backup Media Movement Log.

2.13.4 Back Up, Recovery and Contingency Planning

The objective is to ensure that adequate plans exist for backing up critical network for the timely and logical recovery of information.

(a) Obtain and review a copy of the backup and recovery procedures
(b) Evaluate the procedures used to back up the network to ensure proper backed up as needed
(c) Consider whether retention of backups
(d) Review evidence of successful recovery testing
(e) Review the installation's procedures for recovering a lost disk on the server

(f) Determine the network availability/criticality needs if there is an uninterrupted power supply (UPS) attached.

2.14. Virus Management Policy

2.14.1 Objective

To minimise business disruption by protecting computer resources against intrusion and damage by viruses, spyware and other malware.

2.14.2 Scope

This policy covers all IT systems and IT infrastructure components of .

2.14.3 Policy statements

Virus Management

(a) Antivirus software shall be installed and be kept operational on all servers and workstations, including laptops, by IT staff to protect against virus attacks.
(b) Antivirus software shall be kept updated with latest virus definitions at all times.
(c) Virus scans shall be performed on a periodic basis to detect and remove any virus.
(d) Anti-spyware shall be installed on the servers and workstations to protect against threats other than viruses.

2.15 Internet Usage Policy

Objective

is committed to developing appropriate technology to ensure the efficient and cost effective provision of services. To this end employees are encouraged to develop IT skills including using the email system as a communication tool and accessing the Internet. All use of email and the Internet by employees of must be in accordance with this policy.

The purpose of this policy is to assure that:

a) Users are informed about the applicability of policies and laws to Internet and Electronic mail usage.
b) Internet and Email services are used in compliance with those policies and laws.
c) Users of Email services are informed about those concepts of privacy and security that apply to Email
d) Disruptions to ’s internet, Email and other services and activities are minimised.

Scope

This policy is applicable to

a) All users of Email services who have access to the network
b) Systems and networks owned or operated by .
c) Email in its electronic and printed form.

Internet Usage Statement

a) Users shall not use or access the internet for non-business purposes and restrict personal use to minimum limited to educational and knowledge and news.
b) Users must be aware that accepts no liability for their exposure to offensive material that they may access via the Internet.
c) reserves the right to monitor and review Internet usage of users to ensure compliance to this policy.

2.16 Wireless Security Policy

Objective

To minimise the potential risk of unauthorised access to ’s information systems through wireless access channels by specifying the conditions that wireless infrastructure devices must satisfy to connect to network. Only those wireless infrastructure devices that meet the standards specified are approved for connectivity to ’s network.

Scope

This policy applies to:

a) All employees, students consultants, temporary and other workers at including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of must adhere to this policy.
b) All wireless infrastructure devices, including, but not limited to, laptops, desktops, cellular phones, and tablets, that connect to network.

2.16. Policy Statements

Wireless access requests

(a) Request for wireless connectivity to the 's network should be made by completing a Request for Wireless Connectivity Form (RWCF).
(b) All wireless access holders are subject to the Wireless Access Terms of Use.

2.17 IT Asset Management

Objective

To ensure that all IT assets of are effectively and efficiently controlled, utilised, safeguarded and managed.

Scope

This policy covers the full lifecycle management of IT assets, which includes:

a) Asset Acquisition
b) Maintaining an Asset Register
c) Asset Disposal

2.17.1 Policy Statements

Acquisition of Assets

a) The acquisition of assets is governed by the Procurement Policy and Procedure
b) Request for quotations should be made from a list of approved vendors.
c) ICT department will provide specification of the equipment and systems to be procured
d) The purchase of new equipment or other IT assets above a value of or
e) must be approved by the procurement committee.
f) All other purchase of IT assets should be approved by the Head of Human Resources and .....on the authority limits set out in the Procurement Policy
g) An evaluation and selection report should be prepared and submitted for approval in accordance with the limits set out in the Procurement Policy.
h) All purchase of new equipment or other IT assets should be added to the IT asset register.

Maintaining an Asset Register

(a) The assets register is maintained in accordance with the finance policies and procedures.
(b) All IT assets must be entered in an IT asset register at the time of purchase and details of assets updated as required.
(c) The IT asset register should contain the following details:
    a) Asset ID No.
    b) Asset Description
    c) Brand
    d) Model No.
    e) Serial No.
    f) Purchase Date
    g) Location of Asset
    h) Purchase Value

(d) The Administration should be responsible for maintaining the IT asset register.

(a) A physical inventory of IT assets should be carried out at least yearly and reconciled against the IT asset register. The physical inventory and reconciliation should be signed by the Admininistration and documented.

2.17.2 Asset Disposal

The frequently changing IT environment means that computing equipment (personal computers, laptops and peripherals such as printers) periodically becomes surplus to requirements or reaches the end of its useful life. Equipment with a residual value are subject to be disposed of, all traces of the data contained on the ICT equipment must be securely removed from the equipment prior to their disposal.
The list of ICT equipment that need to be disposed of must be prepared by the Director of ICT and submitted to the asset valuation committee on regularly basis.

Approval for the disposal of an IT asset must be sought using an Asset Disposal Form (ADF).The disposal of an IT asset must be duly recommended by the IT and approved in accordance with the Policy on Disposal of Assets.

Policy Compliance

Compliance Measurement

The University team headed by the Quality Assurance, HR and ICT will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, reports, internal and external audits, and feedback to the policy Users.

Exceptions

Any exception to the policy must be approved by the UTB team in advance.

Non-Compliance

An employee or student found to have violated this policy, violate UTB Values too, may be subject to disciplinary action, up to and including termination of employment and/or suspension.

Thereof, Any concerned person who becomes aware of any violation or suspected non-compliance with the policies in this manual must immediately inform Management, who is responsible for taking any necessary corrective action after investigation.

Any possible non-compliance/violation needs to be reported in a written or electronic form in which the author of the report is identified. The person reporting the violation may request anonymity. Suspected violation must be communicated to the IT.

Policy Management and Update

e) A Custodian (IT) shall be formally designated for the update and maintenance of the IT policy manuals and their contents.
f) The Custodian shall be responsible and accountable for establishing and enforcing standard and consistent procedures to deal with any changes made to the existing IT policy.
g) The policy shall be systematically reviewed by the ITand any Head of Department at least once every 3 years and/or as and when there are IT or business related changes.
h) All changes to the manual shall be requested in an email to the custodian, including the following minimum details:

vi. Date of request
vii. Originator of request
viii. Policy or process name impacted, with corresponding reference
ix. Description of change/update requested
x. Rationale/benefit of the requested change

Localized Policies

- Notwithstanding the broad elements of this policy, campus units may establish or seek to establish complementary policies, standards, guidelines or procedures that refine or extend the provisions of this policy and to meet specific local needs. In any event, such extensions shall comply with university regulations, ordinances and national laws.

Approved by UTB Management Meeting

…….

KABERA Callixte

Vice Chancellor

Date: ……