ARUSHA TECHNICAL COLLEGE

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY AND PROCEDURES

MARCH 2023

LIST OF ACRONMYS AND ABBREVIATIONS

ADS	Active Directory Server
ATC	Arusha Technical College
ATM	Automatic Teller Machine
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
e-Government	Electronic Government
GN	Government Notice
ICT	Information and Communication Technology
IMS	Information Management System
ISO	International Standard Organization
ISP	Internet Service Provider
LPO	Local Purchase Order
NACTE	National Council for Technical Education
PMU	Procurement Management Unit

DEFINITION OF KEY TERMS

i. **Antivirus** is a “protective software designed to defend your computer against malicious software. Malicious software, or "malware" includes: viruses, Trojans, keyloggers, hijackers, dialers, and any other code that vandalizes or steals your computer contents”

ii. **Bandwidth** is the amount of data that can be transferred over a network in a given time period (usually a second). Bandwidth is usually expressed in bits per second (bps), or as some larger denomination of bits, such as Megabits per second (Mbps), or Gigabits/second (Gbps).

iii. **E-learning** is use of information and communication technologies to enhance and support teaching and learning. This definition encompasses e-learning which supports teaching and learning through the provision of online resources to support classroom-based learning, distance learning, and distributed learning models.

iv. **Electronic mail (e-mail)** is a system of world-wide electronic communication in which a computer user can compose a message at one terminal that can be regenerated at the recipient's terminal when the recipient logs in.

v. **Firewall** is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. The integrity of this protective barrier depends on the effective deployment, configuration and capabilities of individual firewall programs.

vi. **Free and open-source software (F/OSS, FOSS)** is software that is, liberally licensed to grant the right of users to use, study, change, and improve its design through the availability of its source code.

vii. **Hardware** is a comprehensive term for all of the physical parts of a computer, as distinguished from the data it contains or operates on, and the software that provides instructions for the hardware to accomplish tasks.

viii. **ICT Assets/Resources** cover all ICT facilities including the College network, all computers, computing laboratories, all associated networks in classrooms, lecture theatres, and video conferencing rooms across the

University, internet access both wired and wireless, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the College), audio visual system including telephone services and voicemail.

ix. **Information and Communication Technology (ICT)** refers to all those instruments, modes, and means through which information or data is captured, processed, stored and transmitted or communicated from one person to another or from place to place

x. **Information management systems** is a computer program (consisting of data storage systems, software and services, providing automated networked storage solutions) that lets one or more computer users create and access data in a database, having extensive transaction processing capabilities.

xi. **Institutional repository** is an online locus for collecting, preserving, and dissemination in digital form of the intellectual output of an institution, particularly a research institution.

xii. **Internet** is a computer network consisting of worldwide interconnected networks of computers that use the standard Internet Protocol (TCP/IP) to facilitate data transmission and exchange,

xiii. **Proprietary software** is a, “computer software licensed under exclusive legal rights of its owner”

xiv. **Software** is a collection of various kinds of programs that are used to operate computers and related devices.

Table of Contents

CHAPTER ONE

INTRODUCTION

1.1 Background

The Arusha Technical College (ATC) formerly known as Technical College Arusha (TCA) was established in 1978 through an agreement of Technical Co-operation between the Government of the United Republic of Tanzania and Government of the Federal Republic of Germany (FRG) which was also known as “West Germany”. The name Arusha Technical College (ATC) came into existence officially from March 2007 when the College was given autonomy through the Arusha Technical College Establishment Order No. 78 of March 2007 under the NACTE Act No. 9 of 1997 which was later revoked and replaced by the ATC Establishment Order GN 302, 2015.

The College has been investing in Information and Communication Technology (ICT) resources to facilitate its core functions of training, research and consultancy services. The use of ICT at the College is increasing in response to the increasing number of students and staff and the need to improve efficiency in service delivery. It is acknowledged that the development, deployment and utilization of ICT within the College, raise a number of challenges in infrastructure, safety and security. Furthermore, the College has to ensure that its ICT resources are used solely for the purposes for which they were intended.

Thus, establishment of ICT Policy and Procedures is to ensure planning, development, deployment and utilization of ICT resources and services at the College effectively support its training, research, consultancy and administrative activities.

1.2 ATC's Vision and Mission

1.2.1 Vision

The vision of ATC is a society with practical knowledge, skills and attitude for sustainable development.

1.2.2 Mission

The mission of ATC is to solve society demand-driven needs by providing competence -based training, research and consultancy.

1.3 Rationale of the Policy

The College invests in ICT resources and services to facilitate its core functions of training, research, and consultancy. Effective support of the College core functions and achievement of its vision and mission requires complying with relevant legal, contractual, professional, and policy obligations whenever ICT resources are used. The College needs to comply with the National ICT Policy 2016, National e-Government Strategy and the e-Government Standards and Guidelines.

The College operations including students' admission and registration, financial management, examination and certification, human resource management and others depend highly on the effective and efficient use of ICT resources and services, making the College vulnerable to ICT related threats. The business continuity of the College depends highly on the use of ICT resources and services.

In this regard, the College needs a comprehensive ICT policy for the effective and efficient use of ICT resources in supporting its core functions. This policy is also intended to improve efficiency and effectiveness of the College administrative operations.

1.4 Purpose of the Policy

The ICT Policy and Procure aims to ensure planning, development, deployment and utilization of ICT resources and services at the College effectively support its training, research, consultancy and administrative activities. The policy will spearhead this purpose through the following specific objectives:

(i) Ensure reliable, interoperable and sustainable ICT resources and services that supports the core functions of the College

(ii) Develop strategies, rules and guidelines to ensure confidentiality, integrity and availability of ICT resources and services.

(iii) Ensure that ATC is able to continue its core activities in the event of significant information security threats.

(iv) Ensure responsible and accountable use of ICT resources and services in accordance with applicable laws, policies, regulations and guidelines.

(v) Improve knowledge and skills of staff, students and other stakeholders for effective and efficient use of ICT resources and services to support the College core functions.

(vi) Manage timely all risks associated with the use of ICT resources and services at the College

1.5 Scope of the Policy

This policy broadly covers all of the College ICT resources and services – hardware, software, and content; this includes but is not limited to electronic networks, systems, computers, devices, telephones, software, data, files, and all content residing in any of these (referred to as "ICT resources"). This policy applies to all records of the College and to the information in those records, regardless of the form or the location.

The policy is applicable to all ATC staff and students, visitors, officials temporarily assigned some activities at the College as well as providers offering services to ATC, all users of ICT resources owned or leased by the College as well as equipment connected to ATC's ICT infrastructure. It is applicable to all campuses and centres as well as student hostels.

CHAPTER TWO

POLICY STATEMENTS AND PROCEDURES

2.0 Introduction

Arusha Technical College is committed to ensure effective and efficient use of ICT resources that facilitate its core activities of training, research and consultancy and other varied operational and administrative activities involving students, staff members and the public. All these activities will be governed by policy statements as stipulated in this document. Each policy statement is supported by operational procedures that describe what must be done to be in compliance.

2.1 ICT Governance and Management

ICT Governance is an integral part of the College governance and consists of the leadership, organisational structures and processes that ensure that the organisation's ICT sustains and extends the organisation's strategies and objectives.

Effective ICT Governance provides a conducive environment for the alignment of all ICT investments in a rationalized manner that is aligned towards enabling the College meet its goals and objectives. This also contributes to the attainment of value for money, management of risks and effective utilization of ICT resources.

2.1.1 Policy Statement 1

The College shall ensure high level of ICT governance and management for effective development, deployment and exploitation of ICT resources for facilitating the core functions of the College

Operational Procedures

The College shall:

(i) Establish ICT governance and management structures within the College for effective development, deployment and exploitation of ICT resources and services;

(ii) Develop ICT strategic plan that is aligned with and serves the College strategic goals and directions;

(iii) Impose the use of ICT in all its core functions of training, research and consultancy as well as administrative and management functions;

(iv) Ensure availability of adequate and skilled ICT human resources in terms of technical, academic and administrative staff;

(v) Ensure that staff and students have access to ICT resources to facilitate their day-to-day activities;

(vi) Ensure availability of appropriate ICT resources to meet the needs of the College community; and

(vii) Ensure that ICT Risk Management periodically done where by ICT risk assessment should be performed to access and analyse all risks relating to College's ICT critical systems. The results of such assessment shall be documented and subject to mitigating measures.

2.1.2 Policy Statement 2

The College shall ensure availability of adequate financial resources acquire and manage ICT resources.

Operational Procedures

The College shall:

(i) Allocate in its annual budget adequate fund for regular acquisition and management of ICT resources;

(ii) Seek partnerships and collaborations as way to access resources for financing ICT services and resources;

(iii) Develop short and long-term demand driven ICT programmes for the purposes of mobilizing additional resources to sustain ICT services and resources; and

(iv) Write competitive fundable proposals to solicit fund for supporting ICT services and resources.

2.1.3 Policy Statement 3

The College shall monitor and evaluate all usage of ICT resources and services to ensure applicability, safety and security.

Operational Procedures

(i) Collect data and report regularly on the use of ICT resources and services at the College;

(ii) Establish proper automated procedures to ensure internal incidents are tracked and resolved timely;

(iii) Conduct internal and external audits of all ICT resources and services as part of its legal requirements and business processes;

(iv) Ensure that reports on the usage and utilization of ICT resources and services are reported to the College Management and recommendations are implemented timely; and

(v) Ensure that observations of the internal and external auditors and the decisions of the College Management, ICT Steering Committee and Governing Board are complied with by the Departments/Units/Sections and users.

2.1.4 Policy Statement 4

The College shall ensure that all users are aware of the provisions set forth in the policy document for compliance.

Operational Procedures

The College shall:

(i) Ensure that the ICT Policy and Procedures is available both in hardcopy and softcopy in the College network for all users of ICT resources and services to be familiar with it;

(ii) Prepare leaflets summarizing key policy provisions targeting end users;

(iii) Publish this policy to the College community through official College website and other communication media;

(iv) Set procedures for reporting incidents of actual or potential threat of the violation of the policy and procedures prescribed therein; and

(v) Ensure that appropriate disciplinary measures are taken in case of violation of the policy as per government and ATC laws, regulations and guidelines.

2.2 ICT Equipment and Infrastructure

ICT equipment and infrastructure are essential in enabling exchange of information and providing secure access to different applications. ICT equipment and infrastructure consists of network devices, computer servers, security devices, workstations, laptop computers, printers, scanners, digital cameras, storage devices, power back-up, operating facilities and supporting platforms like operating systems and databases.

Optimal use of ICT equipment in supporting the College business operations depend on deployment and management practices.

2.2.1 Policy Statement 5

The College shall continue to improve its data communication networks and ensure availability of appropriate hardware and software in order to meet the needs of the College Community.

Operational Procedures

The College through ICT Unit shall:

(i) Ensure availability of appropriate software and hardware to meet the needs of staff and students;

(ii) Ensure availability of alternative sources of power for smooth running of ICT services;

(iii) Establish common set of standards for hardware, system architecture, and software (proprietary as well as free and open source) for use at the ATC;

(iv) Ensure that ICT resources and services are well maintained and regularly upgraded and updated to meet the set objectives;

(v) Establish an active directory server (ADS) for ATC staff and students to enhance real time storage of data;

(vi) Establish a remote server system for real time storage of ATC data and documents;

(vii) Ensure all departments, units, sections, workshops and laboratories have adequate ICT equipment to operate their activities effectively; and

(viii) Establish modalities for sharing ICT equipment at the College in order to reduce costs and avoid duplication of efforts.

2.3 Internet and E-mail Services

The College has network connectivity that enables employees to browse the internet for information and communication services. The College encourages staff and students to use internet and e-mail services to facilitate business operations. Responsible use of internet and e-mail services is the key for the effective implementation of the core functions of the College.

2.3.1 Policy Statement 6

The College shall ensure there is sufficient bandwidth to meet the requirements of the entire College community.

Operational Procedures

The College shall:

(i) Ensure that all Internet Service Providers (ISPs) engaged by the College guarantee availability of adequate backup so that internet connectivity is available at all times and on the agreed bandwidth;

(ii) Bandwidth usage is restricted to ensure that access to critical information, research and online educational resources are always optimal;

(iii) Explore viable strategies to reduce bandwidth costs for the institution

(iv) Ensure that the bandwidth is restricted from unauthorized persons and services;

(v) Monitor the bandwidth usage through management of network devices to ensure optimal functioning and security;

(vi) Perform periodic Assessment of bandwidth requirements to meet needs of the College;

(vii) Ensure all software used to access the internet shall be part of the standard software suite or approved under the ISO standard;

(viii) Ensure that Internet access software shall incorporate the latest security updates provided by the vendors;

(ix) Ensure all internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited;

(x) Ensure internet access traffic through the College ICT infrastructure shall be subject to logging and review;

(xi) Ensure secondary internet link is available for continuing internet access; and

(xii) Ensure that College internet access infrastructure shall not be used for personal solicitations, or personal commercial ventures.

2.3.2 Policy Statement 7

The College shall ensure availability of a secure and reliable e-mail system and provide each staff an e-mail address under the College domain name structure

Operational Procedures

The College shall:

(i) Develop email communications standard operating procedures for the College staff;

(ii) Ensure that the College e-mail system is protected from physical and non-physical threats;

(iii) Provide mechanisms to control the amount of unsolicited emails that users receive;

(iv) Provide mechanisms to intercept emails that contains viruses;

(v) Ensure postings by users from the College email address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly the user's and not necessarily those of the College, unless posting is in the course and within the scope of official duties. This means that e-mail to be sent or received through the College e-mail address shall have the following features:

(a) Courteous and polite

(b) Protect other's right to privacy and confidentiality

(c) Do not contain obscene, offensive or slanderous material

(d) Do not unnecessarily or frivolously overload the email system (e.g. spam or junk mail)

(e) Do not carry viruses or any other malware contents

(vi) Ensure that when an employee leaves the College, the password of his/her e-mail account shall be changed immediately so that he/she cannot access the data/mails stored in the mail box.

2.4 ICT Security, Safety and Confidentiality

The College is committed to all ICT resources are protected from unauthorized or unintended access, modifications, disclosure or destructions. The level of protection shall commensurate with the risk exposure and with the value of the information and of the ICT resources. The general objective of protecting ICT resources is to ensure the College achieve its mission and strategic objectives.

The College must also take reasonable steps to ensure that ICT resources are handled with due regard for privacy and confidentiality concerns.

2.4.1 Policy Statement 8

The College shall ensure that all ICT resources and services are protected and secured from any form of unauthorized access and use

Operational Procedures

The College shall ensure that:

(i) All ICT devices (including servers, desktops, laptops and mobile devices such as smartphones and tables) storing or processing College information must meet device protection requirements;

(ii) All devices connecting to or installed on a non-guest ATC network or authenticating to ATC applications must be configured for secure operation, including non-default unique passwords/credentials that limit access to authorized individuals and services, proper registration of the device on the network, current and supported operating system;

(iii) The information stored on the device must be protected against access if the device is lost, stolen, or recycled/reissued to another user. All mobile ICT resources that may be used to store or access ATC information, including accessing information management systems and e-mail, must be securely configured, including encryption of data stored on the device, where this feature is supported;

(iv) All College computing devices are protected against malicious software through the installation of antivirus and firewall software;

(v) All information systems that are in-house designed and developed or acquired must have ICT security controls to safeguard the integrity, confidentiality and continual availability throughout the entire life cycle;

(vi) People responsible for the operation and management of servers and other ICT resources that store or process College information must have the skills, experience and/or training needed to implement security requirements; and

(vii) Regular backups and any other security measures are taken to ensure that the data is saved is protected and can be relied upon in the event of loss of online data.

2.4.2 Policy Statement 9

The College shall ensure that all users are responsible for protecting their ATC passwords and other credentials from unauthorized access and use

Operational Procedures

The College shall ensure that:

(i) Passwords used on all systems for ATC business should be of sufficient length and complexity to reasonably protect them from being guessed by humans or computers. Further, users must leverage multi-factor authentication (two-step verification) wherever supported;

(ii) Systems that manage user passwords and other access credentials must be designed in such a way that the passwords are not retrievable by administrators;

(iii) Different passwords must be used for ATC and non-ATC accounts. Passwords for College accounts shall noy be used for non-college access such as personal ISP account, Web Mail, and Bank ATM;

(iv) Users' passwords and other access credentials must never be shared;

(v) All passwords and other access credentials must never be stored in plaintext and must not be stored directly in scripts or configuration files;

(vi) Passwords must be changed immediately if there is suspicion of compromise. The ICT and Statistics Unit shall be alerted immediately to investigate the incident, if it affects the College critical information systems or processes;

(vii) Defence procedure, password cracking or guessing tools may be performed on a periodic or random basis by the relevant staff of the ICT and Statistics Unit or its delegates. If a password is guessed or cracked during one of these scans, the affected user shall be required to change the password immediately;

(viii) Servers and applications that manage passwords must force the setting of a complex password. Further, they must enforce multi-factor authentication where technically possible. Strong and complex passwords must have the following characteristics:

a) Are at least eight (8) alphanumeric characters long

b) Contain at least one number (i.e., 1,2,3,4,5,6,7,8,9,0), at least one special character (i.e., @, #, $, %, &, *!) and upper and lowercase characters (a-z, A-Z)

c) Are not based on personal information, or names of family, among others

d) Are configured to expire after every 30 days and one is required to change to a new password

(ix) User password must be blocked after five (5) failed Login attempt threshold;

(x) Default passwords must be changed and generic accounts must be disabled or removed before the server or application is put into use;

(xi) Mechanisms for users to set or change passwords must be secure. Systems that manage passwords must be configured securely; and

(xii) User passwords must be changed immediately when an employee leaves the College to prevent access to systems and applications.

2.4.3 Policy Statement 10

The College shall ensure that all critical systems, and systems and locations where College information is stored are accurately identified, physically secure and protected against improper access

Operational Procedures

The College through the ICT and Statistics Unit shall ensure that:

(i) Server operators must be able to identify a responsible party, known as the business application owner, for each application on the server and the data classification level of the information that the application stores and processes;

(ii) Communications between servers or applications and client machines must be protected, whether these servers are managed directly by ATC or via contract with a third-party service provider for ATC's use;

(iii) Users must only be permitted to access a server or application after their current business need for access has been established;

(iv) All servers must run malware detection and endpoint detection and response software with up-to-date signature files;

(v) Server operators must not knowingly permit shared user account credentials;

(vi) Servers or applications must implement a mechanism that inhibits password guessing attacks on user accounts if the server or application does its own authentication;

(vii) Servers must be protected from improper network-based access;

(viii) Confidential information on servers and backup media must be protected against access in the case of physical theft or loss;

(ix) Administrative functions on servers and applications must be logged. All logs must be recorded in both hard copy and/or stored online;

(x) The logs must periodically be reviewed for anomalous behavior;

(xi) Server operators must take reasonable actions on a regular basis to ensure that their systems are not vulnerable to attack;

(xii) Offsite data recovery site shall be available;

(xiii) Outbound traffic from servers must be limited to that required to properly operate the service;

(xiv) Servers must be kept in secure locations and properly inventoried. The server room must have:

(a) Air cooling system either air condition or electrical fan installed
(b) Smoke detectors and fire management system
(c) Proper cabling arrangements, so that they may not contact humidity or water and cause electric shock
(d) Materials which cannot catch fire easily
(e) Biometric devices are installed

(xv) Back-up plans, with the schedule of the general regular back-up pattern for the key College systems, shall be documented;

(xvi) Back-up must be tested to check accuracy and completeness of data; and

(xvii) Access to the computer server rooms shall be restricted to the authorized College staff only.

2.4.4 Policy Statement 11

The College shall provide a formal approach to management of change enabling individual changes to be applied in a controlled and consistent manner.

Operational Procedures

The College shall ensure that:

(i) Changes to the system are authorized by the College Rector or senior management officials depending on the types of changes;
(ii) A change request is submitted to the College Rector giving details of the changes to be done such as description of the change, date and time, impacts, and the main contact person;
(iii) Changes that will impact the entire ATC community will be communicated officials through various channels of communication; and
(iv) All changes are documented after their implementation, whether the implementation was successful and/or issues resulting from the change.

2.5 Information Management Systems and Website Management

Information Management Systems (IMS’s) are systems that collect, monitor, manage, analyse, and disseminate information about various inputs, processes and outcomes relating to the College business operations. They help the College to plan, manage and strategize to implement work processes to execute its business operations effectively and efficiently. Thus, the acquisition and management of these information systems needs to be well planned and coordinated to ensure optimal use of resources, systems interoperability and valued services. In this way, policy provisions are needed to ensure system acquisition; development, use, maintenance and upgrades are managed properly.

Website is a powerful means of communicating with the internal and external College stakeholders. It is also an important tool for marketing and expression of the College brand. It is therefore important to properly manage website activities.

2.5.1 Policy Statement 12

The College shall systematically develop, procure, adopt and adapt information management systems to facilitate its business operations

Operational Procedures

The College shall:

(i) Promote and encourage the use of information management systems to manage the key functions of the College and its related functions;

(ii) Ensure that appropriate software and platforms are developed, acquired or customized for managing different College functions;

(iii) Ensure that all acquired software bare legitimate licences and accompanied by technical documentation and user manuals;

(iv) Ensure that all acquired, developed or customized software comply with the user's requirements, e-government guidelines and other relevant standards;

(v) Ensure that are in-house developed software are managed by the ICT and Statistics Unit and patented according to intellectual property laws and regulations of the United Republic of Tanzania;

(vi) Ensure that proper procedures are followed during development of in-house software and documentation is maintained for reference and verification; and

(vii) Train staff and students on the use of various College information management systems.

2.5.2 Policy Statement 13

The College shall ensure that website content must be clear, accurate, up-to-date and relevant to its vision, mission and functions.

Operational Procedures

The College through the ICT and Statistics Unit in collaboration with the Public Relation Office shall:

(i) Ensure that all contents to published on the College website are approved by the Deputy Rector-Academic, Research and Consultancy (DR-ARC);

(ii) Ensure that contents are evaluated, revised, proofread and edited by another member of staff before being uploaded to the website;

(iii) Ensure that any content uploaded does not include any breach of copyright or other intellectual property rights;

(iv) Ensure that the College website is regularly updated and maintained by the College Public Relation Officer in collaboration with the Head of ICT Unit;

(v) Ensure that the College website is accessible to all internal and external stakeholders;

(vi) Ensure that the College Public Relation Officer prepare monthly, quarterly and annual reports summarizing website updates done; and

(vii) Ensure that the content of third-party websites linked to the College website are relevant, appropriate and operating effectively.

2.6 ICT Procurement, Maintenance and Disposal

The procurement management of ICT resources include all the activities for acquisition, storage, usage, maintenance and disposal of ICT resources. Effective and efficient operations of the College activities depend on procurement management of ICT resources. Thus, there is a need to ensure that user departments' ICT assets and services and properly acquired, maintained to guarantee quality, value for money and avoid other associated risks.

2.6.1 Policy Statement 14

The College shall procure ICT resources and services according to the needs of users in accordance with the laws, regulations and policies governing the procurement processes in the United Republic of Tanzania.

Operational Procedures

The ICT and Statistics Unit shall:

(i) Assist users to prepare technical and performance specifications for procuring ICT tools, equipment and services according to their needs;

(ii) Establish standard procedures for the identification, evaluation and selection of appropriate hardware and software (proprietary and free and open-source software);

(iii) Ensure that requests for ICT assets are submitted to the Procurement Management Unit via the ICT Unit in accordance with the current ordering processes and procedures;

(iv) Collaborate with the Procurement Management Unit (PMU) to identify reputable companies or registered suppliers and providers of ICT tools, equipment and services;

(v) Not approve or proceed without adequate and suitable further justification, the procurement of ICT assets that do not comply with the requirements of the College plans, policies and standards;

(vi) Inspect the delivered of goods and services against the Local Purchase Order (LPO) to examine and test the compliance of the goods to technical and performance specifications;

(vii) Update the minimum specifications of all ICT facilities to meet the demands of the latest technologies to fulfil the needs of the College community; and

(viii) Acquire volume licenses for appropriate software in accordance to the needs of the University community.

2.6.2 Policy Statement 15

The College shall ensure that all procured ICT assets are managed properly in accordance with their legal, regulatory, contractual or licencing obligations.

Operational Procedures

The College shall:

(i) Develop a database for ICT assets/assets management system for proper record management;

(ii) Ensure that all ICT assets procured or acquired through projects or research collaborations are registered in the asset management system/database of ICT assets;

(iii) Ensure that all ICT assets are assigned to individual users or to a department who will be held responsible for their care and security at all times whether they are in use, storage or movement;

(iv) Ensure that users must always contact the Head of ICT Unit if they need to move, reassign or return ICT assets;

(v) Conduct regular inventory checks through the Head of ICT Unit for management reporting; and

(vi) Update and maintain the accuracy of the asset inventory as soon as change is made (including office moves, reports of lost or stolen equipment and disposals).

2.6.3 Policy Statement 16

The College shall ensure that all ICT resources are regularly and adequately administered and maintained to ensure they remain fit for purpose and compliant with the licenced conditions of use during their entire lifecycle.

Operational Procedures

The College shall:

(i) Ensure that ICT resources are deployed and utilized in a way that is deemed most effective for addressing the College needs and objectively demonstrate value for money;

(ii) Ensure that all request to install unapproved software on devices or install additional approved hardware on to a device are made to and approved by the Head of ICT Unit;

(iii) Administer the control and security of ICT resources held in stock for issuing and waiting reissue or disposal;

(iv) Establish a database for all ICT assets within the College and promote proper management and easy retrieval of ICT assets and facilities; and

(v) Establish regular procedures for identifying faults in ICT resources through ICT Unit and prepare maintenance plan that has to be approved by the Deputy Rector – Finance, Planning and Administration.

2.6.4 Policy Statement 17

The College shall ensure that ICT assets which are no longer needed or required to be kept are properly disposed in accordance with the laws, regulations and policies governing the disposal processes in the United Republic of Tanzania

Operational Procedures

The College shall:

(i) Ensure that all ICT assets which have proposed for disposal are returned to the ICT Unit in order to assessed for proposal disposal. Asset which is destroyed, broken beyond repair or for which the repair is deemed by the ICT Unit as not cost-effective, will be properly disposed by the College;

(ii) Ensure that data holding components or storage devices are completely destroyed or wiped before disposal to prevent unauthorized access to the College data;

(iii) Establish a centralized backup and archive system to store important data from obsolete or decommissioned ICT equipment;

(iv) Collaborate with the Procurement Management Unit (PMU) ensure ICT equipment are disposed based on prevailing Government Guidelines for disposal of ICT assets; and

(v) Update the ICT assets inventory once the equipment are disposed.

2.7 Staff Training and Capacity Building on ICT

ICT resources are evolving every time due to speedy technological changes. The College staff need to be equipped with adequate and updated knowledge, skills, and experience to keep up with the changing and emerging technologies. ICT training and capacity building is necessary to ensure effective and efficient use of ICT resources to support business operations.

2.7.1 Policy Statement 18

The College shall ensure that people responsible with the development, deployment and utilization of ICT resources to support its business operations must have knowledge, skills, experience and/or training for effective use and management of ICT resources.

Operational Procedures

The Head of ICT and Statistics Unit in collaboration with the Director of Human Resources and Administration, Head of Departments/Units/Sections shall:

(i) Conduct needs assessment to identify training needs for ATC staff on the development, deployment and utilization of ICT resources;

(ii) Develop a continuing training plan for ATC staff on ICT especially on emerging technologies;

(iii) Provide relevant learning materials on the effective use of ICT resources and emerging technologies to ATC staff;

(iv) Ensure that ICT Unit staff attends local and international ICT workshops and conferences to enhance their knowledge and skills; and

(v) Utilize the existing partnership and seek new partners to support life-long learning in ICT and to build the capacity of staff.

2.8 Business Continuity Management

College business operations are increasingly dependent on the use of ICT resources. Adequate measures shall be in place to manage foreseen and unforeseen events (natural disasters, technological failures or human errors) to ensure business continuity. Business continuity management need to be well planned and implemented to minimize the impact on business operation to an acceptable level and facilitate quick recovery of information systems.

2.8.1 Policy Statement 19

The College shall establish and implement processes to ensure that ICT resources that support business operations are available and accessible all the time.

Operational Procedures

The College through the ICT and Statistics Unit shall:

(i) Develop Business a Continuity Plan (BCP) and ICT Disaster Recovery Plan (DRP) with well-defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO0 for all critical information systems to ensure the ability to recover from failure or unexpected interruption;

(ii) Locate resources for disasters management and regularly test the IT Disaster Recovery Plan to ensure preparedness, compliance and provide assurance on the continuance of key business functions in the event of a disaster as directed by the Government;

(iii) Conduct Business Impact Analysis on critical business operations to refine the recovery requirements; and

(iv) Regularly review and update Develop Business a Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

2.9 Responsible Use of ICT Resources and Services

Members of the ATC community are increasingly dependent on the use of ICT resources and services to perform College business operations. Everyone at the College is responsible to ensure ICT resources are properly used as set out in policy statements and operational procedures.

2.9.1 Policy Statement 20

The College shall ensure that all members of the ATC community use ICT resources and services in accordance with applicable laws, with College policies, and in ways that are responsible, ethical and professional.

Operational Procedures

The users of ATC ICT resources and services are:

(i) Observe all stated policy statements and operational procedures in this policy and other related policies, laws, regulations and guidelines

(ii) Restricted to use ATC ICT resources and services to College business and incidental personal use that may not interfere with ATC work or may result in additional direct cost to ATC

(iii) Prohibited not to take unauthorized actions to interfere with, disrupt, or alter the integrity of ATC ICT resources and services

(iv) Prohibited to destruct, alter, or disclose without authorization of data, programs or other content that belongs to others but that is accessed through ATC ICT resources

(v) Obliged to provide accurate, reliable information to authorized recipients and to preserve vital records

(vi) Prohibited from unauthorized interception of email, electronic communication or other records without the consent of the individuals or authority having custody of them

(vii) Prohibited to use illegal copies of copyrighted software, store such copies on the desktops, or transmit them over networks

2.9.2 Policy Statement 21

The College shall ensure that ICT resources and services are effectively used by individuals with special needs

Operational Procedures

The ICT and Statistics Unit shall:

(i) Strive to provide specialized ICT technologies and support needed for individual with physical challenges;

(ii) Develop modalities to receive feedback from users of ICT that are physically challenged in order to improve their services; and

(iii) Ensure that ICT resources and services are provided to all members of the College community without any form of discrimination or harassment.

2.10 Third-Party Products and Services Management

The College can acquire or provide access to its ICT resources to external organizations or individuals as part of their contractual terms. Special restrictions must be in place for management of third-party products and services. Management of third parties include issues on third party verification, service level agreements, outsourcing, cloud computing services, equipment leasing, maintenance and support services, and lastly issues pertaining to Internet Service Providers (ISPs). Members of the College community and external organizations or individuals are required to abide by the restrictions imposed by the policy, law or by signed contracts.

2.10.1 Policy Statement 22

The College shall establish procedures for vetting, verifying, granting of restrictive access and registering all third parties before being allowed access to any of the College's ICT resources.

Operational Procedures

The College through ICT and Statistics Unit shall ensure that:

(i) All third-party access to the computer rooms is scheduled to occur during regular working hours. If this is not possible, a focal point person from the ICT Unit will be scheduled after hours to accompany the third party;

(ii) Third party and its agents comply with all applicable ATC standards, agreements, practices and policies;

(iii) Each third-party onsite employee acquires ATC ID badge that must be displayed at all times while on the premises. The badge must be returned to ATC upon termination or completion of a contract; and

(iv) Third-party agreements and contracts must specify:

(a) The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software.

(b) The ATC information that the third party should have access to.

(c) The minimum-security requirements that the third party must meet (i.e. method for remote access).

(d) How ATC information is to be safeguarded by the third party. Signing of a non-disclosure agreement (NDA) is typically required.

(e) Strict use of ATC information and information resources for the purpose of the business agreement by the third party. Any other ATC information acquired by the third party in the course of the contract cannot be used for the third-party's own purposes or divulged to others.

(f) Feasible methods for the destruction, disposal, or return of ATC information at the end of the contract.

2.10.2 Policy Statement 23

The College shall ensure third parties protect the information and systems to which they have access.

Operational Procedures

The College shall ensure that:

(i) Written contracts and appropriate riders are executed with all vendors and other third-parties who collect, process host or store information;

(ii) It conducts appropriate due diligence on third parties that will store or have access to ATC information or systems;

(iii) Each third-party employee that has access to ATC sensitive information shall be cleared by signing confidentiality and non-disclosure forms for handling that information; and

(iv) All third-party employees are required to comply with all applicable auditing regulations and ATC auditing requirements, including the auditing of the third-party's work.

CHAPTER THREE

POLICY ADMINISTRATION

3.1 Introduction

Successful implementation of the ICT Policy and Procedures depends on the College administrative structures that are in place to develop tools for operationalizing, enforcing, monitoring and evaluation to ensure desired outcomes.

3.2 The College ICT Steering Committee

The Committee shall ensure among other things, the ICT plans, investment decisions and usage at the College are strategically aligned, cost effective, value driven and delivered timely and within budget.

3.2.1 Roles and Responsibilities of the Committee

The roles and responsibilities of the ICT Steering Committee are:

(i) To ensure alignment of ICT with College business needs so that ICT initiatives and services facilitate achievement of the College strategic objectives

(ii) To review and provide advise on ICT investment portfolio and priorities with a view of attaining value delivery

(iii) To ensure all ICT related risks are properly managed, this includes reviewing and approving institutional disaster recovery plan and ensure its effective implementation

(iv) To ensure optimal resource utilization in ICT initiatives implementation, including proper management of ICT infrastructure, human capital and finance

(v) To undertake continuous monitoring and evaluation of institutional ICT projects to ensure anticipated benefits are realized

(vi) To approve any institutional ICT subcommittee as may, from time to time, be constituted and address specific ICT related matters

(vii) To ensure e-Government guidelines and standards are implemented by the College in order to meet compliance requirements

(viii) To prepare and submit quarterly e-Government progress reports to the e-Government Authority

(ix) To perform such other functions as may be directed by the College Rector

3.2.2 Members of the College ICT Steering Committee

The College ICT Steering Committee shall be by the College Rector (Accounting Officer) as the Chairperson and the Head of ICT and Statistics Unit as the Secretary to the committee. The Committee shall constitute of the following members:

(i) The College Deputy Rector – Finance, Planning and Administration

(ii) The College Deputy Rector – Academic Research and Consultancy

(iii) Head of Planning Unit

(iv) Head of Procurement Management Unit

(v) Chief Internal Auditor

(vi) The College Bursar (Chief Accountant)

(vii) Head of ICT Department

(viii) One member from the Ministry of Education, Science and Technology

3.2.3 Meetings of the ICT Steering Committee

The Committee meetings shall be conducted as follows:

(i) Meets once in every three months.

(ii) Two third of the members shall form a quorum for meeting.

(iii) An ordinary meeting of the Committee shall be convened by the Chairperson, and the notice specifying the place, date and time of the meeting shall be sent to each member.

(iv) Where the Chairperson is unable to act by any reason, the Vice Chairman, selected among the members present, shall converne the meeting.

(v) Decisions of the Committee shall be decided by majority of the vote of the members present and in the event of the equality of the vote the Chairperson shall have a casting vote.

(vi) The Committee may co-opt any person whose presence is in its opinion desirable to attend and to participate in the deliberation of the meeting of the Committee and such person shall have no right to vote.

(vii) Members may attend meetings of the Committee by teleconference, videoconference or by similar communication equipment by means of which all persons participating in the meeting can communicate with each other.

3.3 The College ICT and Statistics Unit

There shall be the College ICT and Unit, which shall operate directly under the Office of the Rector. The ICT and Statistics Units shall be a pivotal technical unit responsible for effective development, deployment and utilization of ICT resources and services at the College. It shall maintain close working relationship with the Deputy Rectors, Head of Departments/Units/Sections by keeping them informed on various ICT issues under their respective jurisdictions and by providing them with technical advice on such issues.

The ICT and Statistics Unit shall perform the following functions:

(i) Develop, strategize, promote and oversee the implementation of the ICT Policy and Procedures;

(ii) Provide ICT Helpdesk Support services which include but not limited to:

  (a) Hardware diagnosis on simple faults

  (b) Software installation - Anti-virus and utility programs and maintenance thereof

    (c) Network maintenance and administration - shared resources and documents
    (d) Website improvement and maintenance
    (e) Software system maintenance
    (f) Servers' management

(iii) Maintain inventory register for ICT resources and services used at the College and update the register regularly

(iv) Develop ICT strategic plan that is aligned with and serves the College strategic goals and directions

(v) Impose the use of ICT in all its core functions of training, research and consultancy as well as administrative and management functions

(vi) Ensure that ICT Risk Management periodically done where by ICT risk assessment should be performed to access and analyse all risks relating to College's ICT critical systems. The results of such assessment shall be documented and subject to mitigating measures

(vii) Collect data and report regularly on the use of ICT resources and services at the College

(viii) Ensure availability of appropriate software and hardware to meet the needs of staff and students

(ix) Establish a remote server system for real time storage of ATC data and documents

(x) Establish modalities for sharing ICT equipment at the College in order to reduce costs and avoid duplication of efforts

(xi) Monitor the bandwidth usage through management of network devices to ensure optimal functioning and security

(xii) Develop email communications standard operating procedures for the College staff

(xiii) Ensure that the College e-mail system is protected from physical and non-physical threats

(xiv) Develop Business a Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for all critical information systems to ensure the ability to recover from failure or unexpected interruption

(xv) Conduct Business Impact Analysis on critical business operations to refine the recovery requirements

(xvi) Regularly review and update Develop Business a Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

(xvii) Discharge other functions and responsibilities as stipulated in various provisions of this policy including policy statements and procedures or assigned by the College Rector

3.4 Roles and Responsibilities of the Head of ICT and Statistics Unit

The College ICT and Statistics Unit shall be led by the Head of ICT and Statistics Unit who has to perform the following roles and responsibilities:

(i) Assess the College requirements of ICT resources and services

(ii) Help the Procurement Management Unit in procurement of ICT resources that align with the College plans, user needs and value for money

(iii) Conduct needs assessment to identify training needs for ATC staff on the development, deployment and utilization of ICT resources and services

(iv) Develop a continuing training plan for ATC staff on ICT especially on emerging technologies

(v) Prepare the proof of concept and cost benefit analysis on system change proposal and present the proposed changes to the College ICT Steering Committee and Governing Board

(vi) Implement the recommendations of both internal and external auditors on issues related to the development, deployment and utilization of ICT resources and services at the College

(vii) Implement and enforce measures to ensure security, privacy and confidentiality on the utilization of ICT resources and services

(viii) Manage licences for all applications that are used in various ICT resources and services at the College

(ix) Conduct regular inventory checks for management reporting

(x) Ensure that the College website is accessible to all internal and external stakeholders

(xi) Discharge other functions and responsibilities as stipulated in various provisions of this policy including policy statements and procedures or assigned by the College Rector

CHAPTER FOUR

POLICY OPERATIONALIZATION, MONITORING AND REVIEWS

4.1 Operationalization

The provisions of this ICT Policy and Procedures shall become operational upon being approved by the College Governing Board, and shall remain valid until repealed by the same authority.

The College ICT and Statistics Unit shall oversee the formulation of operational manuals, guidelines, and monitoring and evaluation tools to guide the effective implementation of the approved provisions of this policy.

4.2 Monitoring and Evaluation

Monitoring and evaluation will be an integral component of the implementation of the policy and should be factored into planning. ICT and Statistics Unit will develop Monitoring and Evaluation (M & E) framework to ensure close follow up of the Policy implementation. Relevant indicators shall be developed and be made available to enable stakeholders at all levels monitor and assess ICT development activities on a regular basis.

4.3 Review

The ICT Policy and Procedures document is an evolving document that will be amended from time to time to deal with changes in technology, applications, procedures, legal and social imperatives and perceived risks.

In the event that any statement or procedure is outdated or a need to introduce new statements and procedures arises as a result of the changing College environment, technological changes or any other reason, such amendments will first be discussed and recommended by the ICT Steering Committee and approved by the approved by the College Governing Board. However, the routine /minor changes can be affected with the approval of the College Rector (Accounting Officer).

The entire ICT Policy and Procedures document will be reviewed after every three (3) years.