



**THE STATE UNIVERSITY OF
ZANZIBAR**

**INFORMATION AND
COMMUNICATION TECHNOLOGY
(ICT) POLICY**

2025

Table of Contents

Table of Contents ii

FOREWORD.....	iv
ACRONYMS.....	v
KEY TERMS	vii
INTRODUCTION	1
1.1 Background	1
1.2 Rationale.....	3
1.3 Scope.....	4
1.4 Vision.....	4
1.5 Mission.....	4
1.6.1 The Specific Objectives.....	5
SITUATION ANALYSIS	6
2.1 Introduction.....	6
2.2 Current Performance.....	6
2.2.1 ICT Governance	6
2.2.2 ICT Infrastructure and Use	7
2.2.3 ICT Service Management and Use.....	7
2.2.4 Communication and Media	8
2.2.5 Teaching and Learning.....	8
2.2.6 Information System and Change Management.....	9
2.2.7 Information System Security	9
2.2.8 ICT Skills Capacity Building	10
2.2.9 Data Management.....	10
2.2.10 Emerging Technologies, Innovation, and Electronic Transaction	11
2.3 SWOT Analysis	12
2.4 Stakeholders' Analysis	15
2.5 Focus Areas	19
POLICY OBJECTIVES, ISSUES AND STRATEGIES.....	20
3.1 ICT Governance.....	20
3.2 ICT Infrastructure and Use	20
3.3 ICT Services Management and Use	21
3.4 Communication and Media	22
3.5 Teaching and Learning	23
3.6 Information System and Change Management.....	24

3.7	Information System Security	24
3.8	ICT Skills Capacity Building	25
3.9	Data Management	26
3.10	Emerging Technologies, Innovation, Electronic Transaction	27
	POLICY IMPLEMENTATION FRAMEWORK	29
4.1	The Policy Strategic Linkages	29
4.2	Institutional Framework.....	30
4.2.1	Directorate of ICT Service (DICTS).....	31
4.2.2	Centre for Digital Learning.....	33
4.2.3	ICT Units in Schools and Institutes	35
4.2.4	The Governance Committee.....	35
4.2.4.1	The ICT and Instructional Technology Committee.....	35
4.2.4.2.1	Members of the ICT and Instructional Technology Committee.....	36
4.2.4.2.2	Functions of ICT and Instructional Technology Committee	36
4.2.4.2	The ICT Technical Subcommittee	37
4.2.4.2.3	Members of the ICT Technical Subcommittee	37
4.2.4.2.4	Functions of Technical ICT Sub-Committee	37
4.3	Legal and Regulatory Framework.....	38
4.4	Roles and Responsibilities of other Actors	38
4.4.1	The University Council	38
4.4.2	Deans and Directors.....	39
4.4.3	Departments, Centres and Units	39
4.4.4	Users of ICT Systems	39
4.4.5	Internal Audit Unit.....	40
4.5	Monitoring and Evaluation.....	40
4.6	Risk Management.....	42

FOREWORD

The State University of Zanzibar (SUZA) ICT Policy has been developed and implemented to guide the identification, promotion, and appropriate application of ICT in supporting university functions in alignment with its vision, mission, and strategic plan. The policy not only contributes to achieving the university's objectives but also complies with Zanzibar and Tanzania's legal and regulatory frameworks. Additionally, it links SUZA's operations with global best practices, principles, and guidelines.

The policy is structured to provide all user groups with clear and well-defined roles and responsibilities, along with implementation guidelines on the application of ICT and the delivery and usage of ICT services within the SUZA community. In addition to other themes, the policy addresses ICT sustainability, infrastructure, services, e-learning, Open Educational Resources, bandwidth and resource management, security, Information System (IS) development and acquisition, and digital learning management.

This information is organised into five chapters. The first chapter introduces the policy by providing background information and a situational analysis. The second chapter outlines the rationale, policy scope, mission, and vision. The third chapter specifies the policy's focus areas, while the fourth chapter discusses the legal and regulatory framework. The final chapter covers policy implementation, monitoring, and evaluation.

This policy will be reviewed regularly to keep pace with the rapid advancements in ICT.

Finally, SUZA wishes to express its gratitude for the support provided by the HEET project, the efforts of each member of the ICT policy development team, as well as the diverse contributions of numerous stakeholders in the development of this policy.



Prof. Moh'd Makame Haji
Vice Chancellor

ACRONYMS

AFRINIC	African Network Information Centre
AI	Artificial Intelligence
CAG	Controller and Auditor General
CICTS	Centre of ICT Services
COSTECH	Commission of Science and Technology
DHR	Directorate of Human Resources
DICTS	Directorate of ICT Services
DGSRC	Directorate of Graduate Studies Research and Consultancy
DRS	Disaster Recovery Site
DVC – ARC	Deputy Vice Chancellors Academics Research and Consultation
DVC - PFA	Deputy Vice Chancellor Planning, Finance and Administration
eGAZ	Zanzibar e-Government Agency
ICT	Information and Communication Technology
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LMS	Learning Management System
M&E	Monitoring and Evaluation
MIS	Management Information System

MOOC	Massive Open Online Courses
OER	Open Educational Resource
OSIM	Online Student Information Management
OSS	Open Source Software
PDCA	Plan-Do-Check-Act
PMDU	Procurement Management and Disposal Unit
PRMU	Public Relation and Marketing Unit
RGoZ	Revolutionary Government of Zanzibar
SAN	Storage Area Network
SARIS	Student Academic Register Information System
SCCMS	School of Computing, Communication and Media Studies
SUZA	The State University of Zanzibar
TCRA	Tanzania Communications Regulatory Authority
TCU	Tanzania Commission for Universities
URT	United Republic of Tanzania
VPN	Virtual Private Network
VR	Virtual Reality
ZICTIA	The Zanzibar Information Communication Technology Infrastructure Agency
ZSGRP	Zanzibar Strategy for Growth and Reduction of Poverty

KEY TERMS

Authorisation/ Authorised	Official SUZA approval and permission to perform a particular task.
Application	A computer software package that performs a specific function for an end user.
Asynchronous courses	Courses in which students are not required to participate at the same time as academic staff. These may be print-based or online courses delivered through learning management systems.
Asynchronous method	The student accesses the online learning materials at his/her convenient time; the student chooses when to use the distance learning platform, usually through archived pre-recorded materials.
Bandwidth	A measurement indicating the maximum capacity of a wired or wireless communications link to transmit data over a network connection in a given amount of time.
Blended Learning	A learning mode that combines both online and face-to-face learning processes.
BY (attribution)	The author or creator should be given the credits.
Cloud SaaS	Software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet.
Computer Lab	A dedicated space equipped with computers and other related hardware and software, intended for educational or research purposes
Congestion	A situation when a network is overrun with more data packet traffic than it can cope with.
Code repository	A storage location for code and other software development assets, such as documentation, tests, and scripts.

Copyright	A legal right created by the law of a country that grants the creator of the original work exclusive rights to its use and distribution, usually for a limited time, with the intention of enabling the creator to receive compensation for their intellectual effort.
Confidentiality	Assurance that information is shared only among authorised persons.
Credible sources	ICT platform from recognized academic institutions. Such as MOOCs, Institutional Repository, YouTube, LMS, website, etc.
Digital Signature	A cryptographic technique used to validate the authenticity and integrity of digital messages or documents.
Disaster Recovery Plan (DRP):	A master plan specifically developed for an organisation describing how to deal with the potential disaster to its information systems. Other related terms include business continuity plan (BCP), business process contingency plan (BPCP) or disaster recovery and business continuity plan (DRBCP)
E-learning:	Teaching and learning activities which involve using computers, internet and interactive networks.
Electronic Payment	Transactions made using digital methods, where money is transferred electronically from one account to another.
End-User	A person or other entity that consumes or makes use of any computing-enabled device or appliance.
E-resources	Electronic Materials in digital format accessible electronically.
Error	A human action that produces an incorrect result
Face-to-face learning	Learning that is conducted in a classroom or practical room where a lecturer interacts directly with students daily as per the allocated timetable.
Functional requirement	A requirement that specifies a function that a component or system must perform
ICT Assets	Any computer, software, hardware (servers, systems, networks, computers, data communications, and telephones,) and all other ICT equipment used by and under the control of the agency.

ICT Security Single Point of Contact	ICT staff appointed that delivers advanced threat detection, incident response, and compliance management to ICT Security policy
Information and Communication Technology resources	Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet, and email facilities, software, information systems and applications, account usernames
Information and Communication Technology	The use of computers, telecommunications and office systems technologies for the collection, Processing, storing, packaging and dissemination of information.
Information Security	The preservation of confidentiality, integrity and availability of information.
Information System	A computerized system or software application used to access, record, store, gather and process information.
Integrity	Ensuring the accuracy and completeness of information and associated processing methods.
Log	A record of operating system events. It includes startup messages, system changes, unexpected shutdowns, errors and warnings, and other important processes
Massive open online courses (MOOC)	Online courses that are designed for large numbers of participants around the world, often offered for free and without many qualifications.
Networking	Interconnected computing devices that can exchange data and share resources with each other.
OER platforms	Platforms which SUZA uses in teaching and learning such as the Institutional Repository, LMS, YouTube etc.
Off-the-shelf software	A software product that is developed for the general market, i.e. for a large number of customers and that is delivered to many customers in an identical format

Online learning	Learning where a student and an instructor are being connected through the internet using online platforms, such as Zoom and Meet.
Open educational resources (OER)	Materials that are offered freely for use by teachers and students. The university may adopt and create materials and share freely with the public.
Open-source	Software in which the original source code is made freely available and may be redistributed and modified.
Packets	A small segment of a larger message in computer network communication.
Personal computers	A general-purpose, cost-effective computer that is designed to be used by a single end-user (Example printer, scanner, keyboard, mouse or speaker)
Protocols	An established set of rules that determine how data is transmitted between different devices in the same network.
Detection Systems	monitoring system that detects suspicious activities and generates alerts when they are detected.
Registered Jacks 45 (RJ -45)	It is a widely used type of registered jack connector in Ethernet cables or network devices
Requirements specification	A specification describing the problem area. (Customer requirements specification is usually provided by the customer and contains a description of the required capabilities of a solution from the customer's point of view.)
System:	A set of integrated devices that input, output, process and store data and information.
Student:	Means any enrolled student to the University.

Synchronous courses:	Courses which students and academic staff participate at the same time, but not necessary in the same campus/location. The delivery platform may be through video conferencing, web conferencing and audio conferencing.
Synchronous method	The online or distance education that happens in real-time i.e. all learners learn at the same time, this can be achieved through such technologies Zoom, Skype, Skype or other virtual meeting tools.
Traffic	Amount of data moving across a computer network at any given time.
Threat	A potential cause of an incident that may result in harm to a system or organization.
Third-Party	Any individual or commercial company that has been contracted by the SUZA to provide goods and/or services to SUZA.
UBUNTU	A popular free and open-source Linux-based operating system that is mostly used on a computer or virtual private server.
User:	Any person who utilises a computer lab services. Or Any individual using any of the SUZA's ICT resources.
University:	Unless stated otherwise, in this policy, the University refers to the State University of Zanzibar.

CHAPTER ONE

INTRODUCTION

1.1 Background

The State University of Zanzibar (SUZA) is a state-owned university established by Act No. 8 of 1999 of the House of Representatives of Zanzibar. This Act was later amended by Act No. 11 of 2009 and subsequently re-amended by Act No. 7 of 2016, Act No. 1 Part 4 of 2019, and Act No. 13 of 2020. The last three amendments facilitated the merger of SUZA with other higher learning institutions in Zanzibar. These institutions include the former Zanzibar Institute of Financial Administration (ZIFA), the College of Health Sciences (CHS), the Zanzibar Institute of Tourism Development (ZIToD), the Kizimbani Agricultural Training Institute (KATI), and the Zanzibar Journalism and Mass Media College (ZJMMC).

The State University of Zanzibar (SUZA) is the only university in Zanzibar owned solely by the Revolutionary Government of Zanzibar. As stipulated in Section 5 of the Act, the primary functions of the university include the provision of tertiary education and consultancy services to serve the interests of the Zanzibari community and ultimately contribute to the social, economic, and political development of Zanzibar in particular and Tanzania in general.

SUZA operates under a quasi-autonomous arrangement governed by the University Council, while the Management is responsible for the day-to-day administrative activities. The Vice-Chancellor serves as the Chief Executive Officer and head of administration. The Vice-Chancellor is assisted by the Deputy Vice-Chancellor for Academics, Research, and Consultancy (DVC-ARC) and the Deputy Vice-Chancellor for Planning, Finance, and Administration (DVC-PFA).

By virtue of their positions, the Vice-Chancellor and the Deputy Vice-Chancellors are members of the university's governing board.

SUZA's operations are guided by its vision, which states: *"To be the preferred Higher Institution of Learning and Research in East Africa"*, and its mission, which reads: *"To offer quality and broadly relevant education and research in*

order to develop a knowledge-based society that can tackle the challenges of the 21st century and beyond.”

Information and communication technology (ICT) has made remarkable progress over the past two decades, accelerating the pace of globalisation and expanding access to education. This progress is evident across various sectors, including higher education institutions. SUZA has been embracing technology to provide its community members with access to educational resources, thereby enhancing teaching, learning, and research.

Furthermore, SUZA utilises ICT for administrative purposes, aiming to improve internal operations and service delivery. To maximise these benefits, SUZA should strengthen information sharing through effective and efficient ICT utilisation, facilitating informed decision-making.

SUZA recognises the potential of ICT in enhancing teaching and learning, a priority reflected in its current strategic plan. Additionally, SUZA installs ICT equipment and services to support various academic and administrative processes. However, these developments have largely been carried out in response to specific demands rather than through a holistic approach.

Though SUZA has undertaken many initiatives to improve its service delivery, an ICT policy is needed to provide a reference framework for mapping out ICT strategy and ensuring compliance. An ICT policy facilitates the continuous development and utilisation of ICT in core and support business processes, enhancing operations, service delivery, and good governance. Therefore, it is essential to develop an ICT policy that encompasses all aspects, from core and support business process re-engineering to ICT adoption and utilisation, in pursuit of the University’s strategic objectives.

SUZA comprises a total of ten campuses spread across different areas of the Zanzibar Islands. These campuses are as follows:

1. Tunguu Main Campus – the headquarters, located 14 km south of Zanzibar Town.
2. Vuga Campus – situated within Stone Town.

3. Maruhubi Campus – located approximately 7 km north of Stone Town.
4. Nkrumah Campus – situated around 10 km north of Stone Town.
5. Kizimbani Campus – approximately 14 km north of Stone Town.
6. Chwaka Campus – about 18 km south of Stone Town.
7. Kilimani Campus – roughly 4 km west of Stone Town.
8. Mbweni Campus – located 10 km west of Stone Town.
9. Mnazimmoja Campus – situated within Stone Town.
10. Mchanga Mdogo Campus – approximately 17 km from Chake Chake town on Pemba Island.

SUZA has made significant strides in ICT by installing computing facilities for both teachers and students, as well as establishing a local network and providing internet access. Teaching facilities such as computers, projectors, and management information systems are managed by the Centre for ICT Services, which is responsible for providing ICT services and technical support.

1.2 Rationale

The University's ambition to integrate ICT into the provision of its core services cannot be realised without a purposefully designed ICT framework that aligns with SUZA's vision and mission to achieve its strategic objectives. To this end, SUZA has been investing in information and communication technology (ICT) to streamline its internal operations. However, the increasing reliance on ICT exposes the institution to potential technological risks.

The ICT policy is essential due to the rapid advancements in science, technology, research, and innovation, which are transforming service delivery. Specifically, the policy aims to enhance teaching and learning by promoting the use of educational technology, online learning platforms, multimedia resources, and collaborative tools to facilitate effective knowledge dissemination and acquisition. Furthermore, the University requires ICT initiatives to support research and innovation, improve administrative efficiency through an effective governance framework, ensure data security and privacy, promote the digitalisation of the education process, and foster digital inclusion and accessibility.

From a broader perspective, the policy is necessary to provide a comprehensive framework for managing ICT infrastructure and resources effectively.

1.3 Scope

The policy is designed to align with the university's structure and provides a framework to harness the potential of technology for educational, research, and administrative purposes. It also addresses associated challenges while ensuring the responsible and secure use of ICT resources within the university community.

This policy applies to all ICT-related resources and services provided by SUZA, both within and outside university settings. It establishes key policy directions concerning ICT governance, ICT infrastructure and usage, ICT service management, communication and media, teaching and learning, information systems and change management, information system security, ICT skills capacity building, data management, and matters related to emerging technologies, innovation, and electronic transactions.

The policy reflects the university's commitment and strategic approach to ICT development in alignment with its broader institutional objectives..

1.4 Vision

Leader in leveraging ICT to advance academic excellence, drive research and innovation, and empower staff, students, and the community to excel in digital technology.

1.5 Mission

Enhancing teaching, research, and administration through ICT as well as engaging stakeholders and ensuring data security while promoting digital proficiency, collaboration, and lifelong learning.

1.6 Objective of the Policy

The main objective of this policy is to transform the University into a result-oriented, responsive, and highly efficient institution that effectively delivers ICT services to its stakeholders.

1.6.1 The Specific Objectives

The specific objectives of this ICT policy are to:

- i. Leverage the ICT agenda to play a critical role in shaping the strategic direction of the University.
- ii. Promote responsible and ethical use of ICT resources.
- iii. Ensure widespread use of digitization in academic and administrative functions.
- iv. Encouraging research and innovations in technology development, use, and general work flows.

CHAPTER TWO

SITUATION ANALYSIS

2.1 Introduction

This chapter analyses the current performance in ICT-related matters, the internal and external environment, and the stakeholders' analysis within which SUZA operates. It establishes the foundation upon which the objectives and strategies of the ICT policy are formulated.

2.2 Current Performance

2.2.1 ICT Governance

ICT governance provides a conducive environment for better alignment between SUZA's business operations and technology. It also improves resource allocation, manages risks, and enhances decision-making processes.

Currently, CICTS operates under the Deputy Vice-Chancellor – Planning, Finance and Administration (DVC – PFA) as a university ICT centre that provides services and support in all ICT-related matters. However, its position under the DVC – PFA limits its representation in university management meetings. This structure causes the centre to function as a single unit with restricted decision-making authority regarding ICT functions.

The ICT governance described in this section articulates the structure, roles, responsibilities, planning, control, coordination, and implementation of the ICT policy at SUZA. It also outlines value delivery, strategic alignment, performance management, technology resource management, and risk management.

However, SUZA currently lacks an ICT governance framework, resulting in limited resource management and strategic alignment. Additionally, there is neither a risk management strategy nor guidelines for compliance with regulations and standards. This has a detrimental impact on the efficiency and effectiveness of ICT service delivery in supporting SUZA's core functions. It also hinders the expansion and sustainability of ICT services.

Therefore, it is strongly recommended that CICTS be strategically transitioned into a Directorate of ICT to enhance the effectiveness of ICT service delivery.

2.2.2 ICT Infrastructure and Use

ICT infrastructure is the backbone of SUZA's business operations, enabling information exchange and providing secure access to various applications. It comprises all hardware devices, including network devices, servers, workstations, laptops, storage, backup systems, and network media such as fibre, wireless, and wired connections. Additionally, it encompasses supporting platforms like operating systems and databases.

The primary objective of managing ICT infrastructure is to optimise its operations, ensuring high-quality service delivery and supporting business-relevant functions in alignment with ICT planning and management best practices.

Currently, SUZA does not have a clearly defined ICT procurement policy that outlines comprehensive business and system requirements for acquiring ICT infrastructure. Furthermore, it lacks appropriate software standards to facilitate acquisition and development, ensuring optimal system configuration for usage, maintenance, and disposal.

2.2.3 ICT Service Management and Use

ICT service management concerns the delivery of ICT resources and core business practices in a manner that ensures end users achieve the most desirable outcomes when accessing the entire solution. The primary objective of ICT service management is to support the academic, administrative, and research functions of the University.

At present, there are limited guidelines for service delivery, user training, and the management and utilisation of ICT at SUZA.

Therefore, it is strongly recommended that a strategy be established to ensure compliance with all standards and guidelines governing ICT service management. Additionally, for each ICT service provided, service level

agreements (SLAs) between the providers and SUZA should be implemented to facilitate the continuous improvement of service delivery.

2.2.4 Communication and Media

The SUZA community employs various communication methods and tools, including social media, email, and the university website, to facilitate communication and support its core functions. These tools have proven to be practical and cost-effective solutions for providing and sharing business information with customers and stakeholders. However, managing and maintaining the university website, email services, and social media platforms to meet stakeholders' expectations has been a significant challenge, limiting effective communication. Therefore, it is essential for the SUZA community to exercise proper control over these tools. In this regard, it is recommended that communication and media guidelines be established to enhance effective communication both within and outside the SUZA community.

2.2.5 Teaching and Learning

Teaching and learning are fundamental processes in education, involving transferring and acquiring knowledge, skills, attitudes, and values. To support these processes, SUZA has implemented various methodologies, tools, and techniques to enable academic staff, students, and researchers to share, access, and update high-quality learning materials. Enhancing the university's core functions—teaching, learning, and research—requires careful planning and increased stakeholders' awareness.

However, evidence suggests that these services, including e-learning, Open Educational Resources (OER), teaching equipment, and other facilities, are not being utilised effectively for the university's development. Furthermore, SUZA is in the process of developing an intellectual property (IP) policy.

To foster an optimal teaching and learning environment, it is recommended that the Centre for Digital Learning (CDL) be strengthened, alongside efforts to enhance the use of emerging technologies, e-learning resources, and digital learning platforms. Additionally, the finalisation of the IP policy is crucial to

ensuring that the contributions of staff, instructors, and students are protected, acknowledged, and properly utilised.

2.2.6 Information System and Change Management

Information systems (IS) are software solutions designed for end-users to support university business processes in their daily operations. At SUZA, IS are already in use for admission, examinations, e-learning, library services, accounting operations, and teaching purposes.

Change management, on the other hand, is a structured approach involving a set of processes used to transition from the current state of IS to a desired future state. It encompasses the management of people and processes during changes resulting from the implementation of new strategies, technologies, processes, or organisational structures.

The primary objective of managing applications is to ensure that information systems—whether in use, under development, or being acquired—meet the business requirements of SUZA. Currently, the absence of a formal procedure for system development, acquisition, and control has led to inefficient utilisation and administration of IS. Therefore, formal procedures must be established to create a conducive environment for effective system development, acquisition, and administration. These procedures will also ensure SUZA's compliance with the guidelines and standards set by the governing authority.

2.2.7 Information System Security

Information system security encompasses all the processes through which computer-based equipment, information, and services are protected from unintended or unauthorised access, modification, or destruction within an organisation.

The primary objective of maintaining information system security at SUZA is to implement robust security mechanisms that support its strategic goals, ensure the continuous operation of the information system, and safeguard business performance and services.

Currently, there is no business continuity plan, incident management framework, disaster recovery strategy, backup system, control measures, audit procedures, or other essential security safeguards in place. Therefore, it is imperative to develop adequate protection mechanisms, including virus and spam prevention, internet security measures, infrastructure protection, data protection strategies, a business continuity plan, a disaster recovery plan, and an incident response management plan.

Additionally, all necessary guidelines must be established to ensure compliance with the standards and requirements set by the governing ICT authority.

2.2.8 ICT Skills Capacity Building

Building the ICT skills capacity of university staff is essential to ensuring that technical personnel responsible for managing and supporting ICT infrastructure and services possess the necessary knowledge and expertise to maintain the efficiency, stability, and continuity of ICT systems and equipment. It also involves providing opportunities and resources for individuals to develop their ICT skills, enabling them to utilise technology effectively and efficiently for academic, research, administrative, and innovation purposes.

For a long time, the university has not conducted a skills needs assessment to identify gaps, develop a capacity-building strategy, establish an ICT human resource development plan, or recognise professional qualifications. Therefore, it is crucial to conduct a needs assessment to determine the required quantity and professional expertise of ICT staff and to formulate a comprehensive capacity-building strategy. Additionally, capacity and skills development is necessary for ICT support personnel to enable them to manage routine tasks appropriately and effectively.

2.2.9 Data Management

Data management at the university is a comprehensive discipline that encompasses various processes, including data collection, sharing, ownership, storage, and privacy. These processes are essential to ensuring that data is well-managed, secure, and accessible for decision-making and

research purposes. Effective data management enhances decision-making processes, improves operational efficiency, supports research initiatives, and ensures compliance with data protection regulations. It enables universities to harness the power of data for academic excellence, innovation, and strategic planning.

However, the current practice within the university reveals weaknesses in data management, including a lack of awareness and inadequate procedures for data sharing and management. Given the significance of data management, it is recommended that SUZA establish clear procedures for effective and efficient data handling and raise awareness within the SUZA community to ensure that university objectives are met.

2.2.10 Emerging Technologies, Innovation, and Electronic Transaction

Emerging technologies and innovation are closely related concepts that significantly impact the university's operations. These disruptive technologies facilitate technological transfer, enhance education, research, innovation, and improve consulting services.

The application of emerging technologies at SUZA has been increasing. Staff and students utilise technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Virtual Reality (VR), and others. However, there are currently no guidelines in place to ensure the safe and efficient use of these technologies. Therefore, it is crucial to establish formal directives that promote the responsible and effective utilisation of emerging technologies among staff and students to enhance educational activities, research, and innovation.

Electronic payments, digitally signed documents, and blockchain technology are shaping the way businesses conduct online transactions. However, SUZA does not have an internal guideline outlining procedures aligned with government directives for conducting electronic transactions when acquiring or offering online services. Therefore, there is a need to develop electronic transaction guidelines to facilitate secure and efficient online transactions.

2.3 SWOT Analysis

This section specifically presents the internal and external analysis within which SUZA operates. The environment was assessed by evaluating the university's strengths, weaknesses, opportunities, and threats. The results of the SWOT analysis are displayed in Table 2.1.

Table 2.1: SWOT Analysis

Strengths	Weaknesses
1. The only State owned University in Zanzibar – good public image. 2. The Chancellor of the University is the President of the Revolutionary Government of Zanzibar (RGoZ) 3. Governed by its own Council. 4. Willingness of the Council and Management towards using ICT to improve its operation. 5. Recognition of ICT functions in SUZA structure. 6. Functioning of Centre of ICT services 7. Autonomy to recruit and make changes in organisational structure. 8. Young and trainable workforce. 9. High ICT penetration in the SUZA community. 10. Utilisation of different systems (such as OSIM/SARIS, and LMS) to facilitate University functions. 11. Availability of University website. 12. Good relation with national and international organisations in academic, ICT and development partners (such as TERNET, HUAWEI, UNDP, BADEA, World Bank) 13. Integration of social media in teaching and learning	1. Lack of appropriate ICT Governance framework. 2. Lack of ICT policies, guidelines, procedures and standards. 3. Un-strategic position of Centre of ICT services. 4. Limited engagement of Head of CICTS in shaping the university business model 5. Lack of adequate manpower to support ICT functions 6. Limited managerial and technical capacity in ICT function. 7. Lack of robust and reliable ICT infrastructure and networking. 8. Lack of integration of electronic records. 9. Obsolete business processes attributed with manual and duplicate recording. 10. Inadequate allocation of resources in ICT development and maintenance. 11. Inadequate ICT procurement and acquisition. 12. Lack of ICT disposal procedure. 13. In-adequate backup and recovery facilities 14. No single point of truth (data fragmentation) 15. Incomplete integration of existing Information systems.

14. Availability of outreach program such as Wastex Lab, DALILA Project	
Opportunities	Threats
1. Good relationship with the government and its governance and regulatory authority (such as e-GAZ, TCRA and CAG) 2. Availability of national broadband infrastructure. 3. Recognition of ICT as one of the national priority areas. 4. Raising awareness by the community in utilisation of ICT services. 5. Demanding of blending online teaching and learning strategies.. 6. Strong collaboration and partnership with development and strategic partners. 7. Availability of Open Educational Resources (OER)	1. Rapid advancement and evolution of ICT. 2. Recognition and adoption of ICT services among universities in the EA region. 3. Human resources mobility within the region. 4. Reliability of services by ICT providers. 5. Insecure supply of technical ICT support. 6. Inadequate fiscal transfer from the Government Fund. 7. Unreliable mains power supply 8. Lack of IP addresses space ownership.

2.4 Stakeholders' Analysis

Based on its operations, SUZA has various stakeholders who interact with ICT services across different campuses. The analysis presented in Table 2.2 identifies the stakeholder groups, their roles, and their expectations regarding the ICT policy.

Table 2.2: Stakeholder's Analysis

Sn	Stakeholders	Role	Stakeholder Expectation
1	University Management	Ensure that ICT initiatives align with the University goals, fostering a supportive and collaborative environment for the effective use of technology in the University setting.	✓ Quality service delivery ✓ Guideline and procedures are strictly followed
2	Academic governing authority (TCU and NACTEVET)	Provide standards and guidelines for ICT adoption and implementation in the academic setting.	✓ Compliance with their standards and guidelines
3	Zanzibar e-Government Agency	Assist in ensuring policy, guidelines and standards are properly implemented	✓ Appropriate governance of ICT activities ✓ Improved quality of ICT services ✓ Compliance with their guidelines and standards

4	The Office of the Controller and Auditor, General Zanzibar	Oversee the policy and actual implementation in order to improve accountability and governance of ICT resources.	✓ Appropriate implementation of the policy and improved ICT governance and performance. ✓ Appropriate governance of ICT activities
5	Head of ICT Services	✓ Ensure the smooth implementation, infusion and diffusion of the policy in the SUZA community. ✓ Ensure ICT policy and guidelines are aligned with university goals.	✓ Provide a framework for managing and optimising ICT resources, mitigating risks to support the SUZA strategic objectives. ✓ Provide a roadmap in handling ICT Directorate. ✓ Efficient and effective ICT services to all SUZA stakeholders.

6	Employee	✓ Use ICT facilities and services in an appropriate and responsible manner. ✓ Ensure that other people do not misuse those ICT facilities and services. ✓ Implement all directives and guidelines stipulated in this policy	✓ Receive training on proper use of ICT resources ✓ Clear guidelines to support their ICT activities. ✓ Fairly support
7	Students	✓ Use ICT facilities and services in an appropriate and responsible manner. ✓ Implement all directives and guidelines stipulated in this policy	✓ ICT facilities are available and running smoothly. ✓ Receive training on the proper use of ICT resources.
8	Visitors	✓ Use ICT facilities and services in an appropriate and responsible manner. ✓ Provide feedback on their experience using the university's ICT services. ✓ Ensure data privacy and security, as well as incident reporting.	✓ ICT quality service delivered. ✓ Immediate support on ICT issues.

2.5 Focus Areas

The University ICT policy covers strategic areas that address the diverse needs and challenges related to information and communication technology. The focus areas collectively address the diverse aspects of ICT within the university and provide a framework for utilising technology effectively, securely, and ethically to support the university's vision, mission and objectives. The following areas are covered by this policy

1. ICT Governance
2. ICT Infrastructure and Use.
3. Communication and Media.
4. Teaching and Learning.
5. ICT Services Management and Use.
6. Information Systems and Change Management.
7. Information System Security.
8. ICT Skills Capacity Building.
9. Data Management.
10. Emerging Technologies, Innovation, and Electronic Transaction

CHAPTER THREE

POLICY OBJECTIVES, ISSUES AND STRATEGIES

3.1 ICT Governance

Objective: *Participatory ICT management for proper decision-making in resource allocation for effective and efficient service delivery.*

3.1.1 Policy issues

- 3.1.1.1 ICT governance framework
- 3.1.1.2 Strategic alignment and resource management
- 3.1.1.3 Risk management
- 3.1.1.4 Compliance with regulation and standards
- 3.1.1.5 Monitoring and evaluation.

3.1.2 Policy Statement

The University shall create an ICT governance framework that will guide proper management of ICT matters in the context of the University's business.

3.1.3 Strategies

- 3.1.3.1 Review University structure, School and Institute to fit ICT governance set up
- 3.1.3.2 Review the university Strategic Plan to align strategic initiatives of ICT matters.
- 3.1.3.3 Develop ICT risk management strategy
- 3.1.3.4 Develop guideline to regulate, manage standard and ensure compliance of ICT issues
- 3.1.3.5 Develop and in place monitoring and evaluation tools of ICT governance indicators

3.2 ICT Infrastructure and Use

Objective: *Sustainable ICT infrastructure that supports University operations on teaching and learning, research, innovation and outreach.*

3.2.1 Policy Issues

- 3.2.1.1 Compliance to Government guidelines
- 3.2.1.2 Asset management
- 3.2.1.3 Networking and connectivity
- 3.2.1.4 Equipment, facilities, and tools

3.2.2 Policy Statement

Objective: *The university shall ensure the proper acquisition, use, maintenance, and disposal of ICT assets to facilitate effective service delivery, sustainability, and value for money.*

3.2.3 Strategies

- 3.2.3.1 Develop users assessment manual on demand, use and maintenance
- 3.2.3.2 Develop a road map for acquisition of required equipment, facilities, and tools.
- 3.2.3.3 Develop maintenance and sustainability plan
- 3.2.3.4 Develop user guide and procedure
- 3.2.3.5 Develop University asset register
- 3.2.3.6 Ensure Compliance with Government procedures on acquisition and disposal
- 3.2.3.7 Conduct periodical assessment on networking and connectivity gaps and requirements.
- 3.2.3.8 Develop guidelines for outsourcing required ICT infrastructure

3.3 ICT Services Management and Use

Objective: *Effective, efficient and reliable ICT services that support University core business functions.*

3.3.1 Policy Issues

- 3.3.1.1 Supporting the proper utilisation of ICT services among the users
- 3.3.1.2 Monitoring and response of ICT services
- 3.3.1.3 User awareness and feedback
- 3.3.1.4 Information Technology Infrastructure Library (ITIL) framework

3.3.2 Policy Statement

The University shall ensure effective user support, response, Service Level Agreement (SLA) and continuous improvement to ICT service delivery.

3.3.3 Strategies

3.3.3.1 Strengthening ICT Services helpdesk

3.3.3.2 Develop service monitoring indicators

3.3.3.3 Create a dashboard to monitor the performance of ICT services

3.3.3.4 Develop sensitization programs to facilitate level of awareness among ICT service users.

3.3.3.5 Adopt ITIL framework in supporting ICT services to users

3.4 Communication and Media

Objective: Use reliable communication platforms for effective communication on service delivery.

3.4.1 Policy Issues

3.4.1.1 Formalisation of E-mail address

3.4.1.2 Website management

3.4.1.1 Social media management and control

3.4.1.2 Content production and management

3.4.2 Policy Statements

The University shall ensure the appropriate mechanism for the use of email, websites, and social media management to support and facilitate proper communication channels and information dissemination within and outside the university.

3.4.3 Strategies

- 3.4.1.3 Develop e-mail guidelines
- 3.4.1.4 Develop social media guidelines
- 3.4.1.5 Adopt government website development guidelines
- 3.4.1.6 Strengthen Public Relations and Marketing Unit to manage content production

3.5 Teaching and Learning

Objective: *Use technology and innovation to facilitate proper teaching and learning environments.*

3.5.1 Policy Issues

- 3.5.1.1 Complete adoption of e-learning teaching methodology.
- 3.5.1.2 Adoption of Online Educational Resources (OER).
- 3.5.1.3 Evaluation of online educational systems.
- 3.5.1.4 Subscription of teaching and learning software that supports research analysis (Smart PLS, Nvivo, Atlas, Evie).
- 3.5.1.5 Fully utilising teaching and learning software (plagiarism, Zoom).
- 3.5.1.6 Acquisition and Management of teaching equipment and facilities (projectors, computer labs, smart boards, video conferencing facilities).
- 3.5.1.7 Center for Digital Learning (CDL) setup.
- 3.5.1.8 Intellectual property.
- 3.5.1.9 Innovative assistive ICT tools and platforms for students and staff with special needs.

3.5.2 Policy Statement

The University shall create conducive teaching and learning environment by strengthening CDL, online teaching methodologies, and ensure timely availability of e-learning resources and teaching and learning software.

3.5.3 Strategies

- 3.5.3.1 Develop CDL guidelines
- 3.5.3.2 Develop e-learning guidelines
- 3.5.3.3 Develop OER guidelines
- 3.5.3.4 Develop teaching equipment and facilities guidelines
- 3.5.3.5 Prioritise resource allocation to required teaching and learning software, including assistive tools for people with special needs.
- 3.5.3.6 Harmonise all teaching and learning software across schools and institutes for implementation.
- 3.5.3.7 Finalise intellectual property policy to support innovation initiative

3.6 Information System and Change Management

Objective: *To ensure flexible, reliable, accurate, and timely delivery of services through effective information systems and change management.*

3.6.1 Policy Issues

- 3.6.1.1 Compliance with eGAZ guidelines.
- 3.6.1.2 Information System change management
- 3.6.1.3 Skills and competencies of Information system

3.6.2 Policy Statement

The University shall ensure compliance with government guidelines and develop a change management strategy to facilitate proper IS adoption.

3.6.3 Strategies

- 3.6.3.1 Adopt government IS guidelines
- 3.6.3.2 Develop change management strategy
- 3.6.3.3 Promote professionalism
- 3.6.3.4 Develop sensitisation program to support the adoption of IS

3.7 Information System Security

Objective: *To ensure confidentiality, integrity, and availability of information systems.*

3.7.1 Policy Issues

- 3.7.1.1 Business continuity plan
- 3.7.1.2 Incident management procedure
- 3.7.1.3 Backup procedure
- 3.7.1.4 Audit and control
- 3.7.1.5 Remote access
- 3.7.1.6 Data confidentiality, integrity and availability (CIA)
- 3.7.1.7 Antivirus and anti-spamming
- 3.7.1.8 Cyber security compliance.
- 3.7.1.9 Access levels, rights and privileges to access ICT services

3.7.2 Policy Statement

The University shall create proper information system security to ensure continuity, integration and availability of IS on service delivery.

3.7.3 Strategies

- 3.7.3.1 Develop a business continuity plan
- 3.7.3.2 Develop incident management procedure,
- 3.7.3.3 Develop a backup procedure
- 3.7.3.4 Develop firewall policy
- 3.7.3.5 Establish and implement audit and control procedure
- 3.7.3.6 Introduce security mechanism for remote access
- 3.7.3.7 Use antivirus and anti-spamming software
- 3.7.3.8 Adopt national and international cyber security compliance.
- 3.7.3.9 Manage segregation of duties to ensure access levels, rights and privileges to access ICT services

3.8 ICT Skills Capacity Building

Objective: *To ensure increased performance and sustainable service delivery.*

3.8.1 Policy Issues

- 3.8.1.1 Need assessment
- 3.8.1.2 Capacity building strategy
- 3.8.1.3 Professional recognition and incentives
- 3.8.1.4 Retention plan

3.8.2 Policy Statement

The University shall implement sustainable capacity-building initiatives to develop a skilled ICT workforce, ensuring effective and efficient service delivery.

3.8.3 Strategies

- 3.8.3.1 Conduct comprehensive capacity needs assessment
- 3.8.3.2 Develop capacity building strategy
- 3.8.3.3 Develop a retention plan
- 3.8.3.4 Review the university's scheme of service to align ICT professionalism with appropriate staff incentives.

3.9 Data Management

Objective: To ensure the reliability, accuracy, completeness, timeliness, and availability of data for effective decision-making.

3.9.1 Policy Issues

- 3.9.1.1 Data availability and control
- 3.9.1.2 Data quality and accuracy
- 3.9.1.3 Users Awareness
- 3.9.1.4 Data life span
- 3.9.1.5 Data protection
- 3.9.1.6 Data storage mechanism
- 3.9.1.7 Data sharing and privacy

3.9.2 Policy Statement

The University shall ensure reliable data management to facilitate proper decision-making in service delivery.

3.9.3 Strategies

- 3.9.3.1 Develop and harmonise data collection tools
- 3.9.3.2 Develop data processing procedures
- 3.9.3.3 Develop sensitization program for data users
- 3.9.3.4 Develop a data management framework to ensure data life span, protection and storage.
- 3.9.3.5 Develop data sharing and privacy guidelines
- 3.9.3.6 Align with the government's data interoperability standards and guidelines

3.10 Emerging Technologies, Innovation, Electronic Transaction

Objective: *To drive transformation and innovation through digital economic services, fostering economic and social development.*

3.10.1 Policy Issues

- 3.10.1.1 Emerging technology strategy
- 3.10.1.2 Innovation strategy
- 3.10.1.3 Infrastructure supporting technology development and innovation
- 3.10.1.4 Networking and collaboration
- 3.10.1.5 Intellectual Property Policy
- 3.10.1.6 Electronic transaction

3.10.2 Policy Statement

The university shall be committed to facilitating technological transfer, encouraging digital transactions, fostering innovation, and positioning itself as a leader in driving positive change through cutting-edge research and education.

3.10.3 Strategies

- 3.10.3.1 Develop emerging technology strategy
- 3.10.3.2 Develop Innovation strategy
- 3.10.3.3 Improve infrastructure supporting technology development and innovation (Internet of Things (IoT), Artificial Intelligence (AI), Virtual Reality (VR), and 5 G)
- 3.10.3.4 Formalise and increase synergy on networking and collaboration
- 3.10.3.5 Develop ICT solution-based ICT project master plan
- 3.10.3.6 Develop electronic transaction guidelines

CHAPTER FOUR

POLICY IMPLEMENTATION FRAMEWORK

4.1 The Policy Strategic Linkages

This policy comprises the University's general vision, mission and objectives as well as policy issues regarding ICT Governance, ICT Infrastructure and Use, ICT Services Management and Use, Teaching and Learning, Information Systems and Change Management, Information System Security, Communication and Media, ICT Skills Capacity Building, Data Management, and Emerging Technology, Innovation, and Electronic Transaction.

The policy is developed as an initiative based on the National Development Vision 2050 and the ICT Policy 2016, which provides a national framework that will enable ICT to contribute towards achieving national development goals; and to transform Tanzania into a knowledgeable society through the application of ICT. By adopting the National ICT policy agenda, the university aims to contribute to the broader development goals set by the country, such as fostering innovation, driving the digital economy, and addressing societal challenges through education and research. This implementation of the policy allows the university to support the national agenda and strengthen its role as a catalyst for progress and sustainable development.

This policy has been developed in alignment with the following documents, including Zanzibar, Tanzanian, and global policies, regulatory frameworks, and legal documents:

- i. Zanzibar ICT Policy (2013).
- ii. Zanzibar's Digital Economy Roadmap (2023–2027), which promotes the expansion of ICT usage in education.
- iii. SUZA Strategic Plan (2019–2023), which highlights the need to strengthen ICT use in delivering administrative and academic functions at the university.

- iv. The CCM Election Manifesto (2020), which emphasises science, technology and innovation (Section 102), and digital economy (Section 103).
- v. The Tanzania Commission for Universities Guidelines for Online and Blended Delivery Modes of Courses for University Institutions in Tanzania (2022)
- vi. Tanzania's National ICT Policy (2016), which promotes ICT expansion in education and establishes guidelines for ICT policy development to meet national demands and facilitate implementation.
- vii. Tanzania's Electronic Transaction Act 2013, which is intended to facilitate electronic transactions and other related matters carried out via Electronic Data Interchange (EDI) or other means of electronic communication methods. It secures the security of electronic signatures, and provides for the use, security, facilitation, and regulation of electronic communications and transactions.
- viii. Tanzania Cybercrime Act 2015, which defines and criminalises computer and network-related crime; provides for the investigation and collection of evidence for computer and network-related crimes; and allows for the admission of electronic evidence for such offences.
- ix. Tanzania's Data Protection Act. 2013, which enhances the protection of personal information processed by public and private entities, as well as adopting information protection principles in order to create minimum criteria for personal information processing.
- x. E-Government Agency Act No. 12 of 2019.
- xi. The Zanzibar Information Communication Technology Infrastructure Act No. 15 of 2020.
- xii. The Inter-University for East Africa, Information and Communication Policy Plan (2020).

4.2 Institutional Framework

The successful implementation of this policy requires a well-defined institutional framework that clearly outlines roles, responsibilities, and processes for policy development, implementation, monitoring, and review.

Establishing a robust institutional framework enables universities to implement, monitor, and adapt their ICT policy initiatives effectively, fostering a conducive digital environment that aligns with the institution's mission, values, and goals. To achieve the intended outcomes of this policy, the following institutional setup is required.

4.2.1 Directorate of ICT Service (DICTS)

The Centre of ICT Services will be transformed into the Directorate. The Directorate of ICT Services at the University will become a centralised department responsible for managing and providing information and communication technology (ICT) services and support to the university community. It ensures that the university's technology infrastructure, systems, and services meet the needs of students, faculty, staff, and other stakeholders. The directorate will be responsible to:

- i. **ICT Infrastructure Management:** The directorate oversees the planning, implementation, and maintenance of the university's ICT infrastructure. This includes managing networks, servers, data centres, telecommunications systems, hardware, and software resources. They ensure that the infrastructure is reliable, secure, and scalable to meet the demands of the university community.
- ii. **User Support and Helpdesk Services:** The directorate provides technical support services to assist students, faculty, and staff with ICT-related issues and inquiries. This can involve operating a helpdesk or service desk to handle user requests, troubleshooting hardware and software problems, assisting with account management, and providing guidance on using university systems and services.
- iii. **Network and Connectivity:** The directorate is responsible for managing the university's network infrastructure, ensuring reliable connectivity, both wired and wireless, across campus. They oversee network design, installation, maintenance, and security measures to support seamless access to internet services and connectivity for all users.
- iv. **Systems and Applications:** The directorate manages and supports various systems and applications used by the university, such as

student information systems, learning management systems, email and collaboration platforms, research databases, and administrative software. They ensure the availability, security, and proper functioning of these systems to support teaching, learning, research, and administrative operations.

- v. **Data Management and Security:** The directorate takes measures to protect the university's data and information assets. They develop and implement data management policies, backup and recovery strategies, data classification, and access control mechanisms. They also ensure compliance with data protection and privacy regulations and establish security measures to safeguard against cyber threats and unauthorised access.
- vi. **ICT Governance and Strategy:** The directorate participates in developing and implementing the university's ICT governance framework and strategy. They collaborate with other departments and stakeholders to align ICT initiatives with the university's overall goals and objectives. They also provide input and expertise on technology trends, innovations, and emerging solutions that can benefit the university's academic, research, and administrative functions.
- vii. **Training and Capacity Building:** The directorate organises and conducts training programs and workshops to enhance ICT skills and digital literacy among students, faculty, and staff. They provide resources and support for professional development in areas such as educational technology, research data management, cybersecurity awareness, and the effective use of ICT tools and applications.
- viii. **Vendor Management and Procurement:** The directorate oversees relationships with ICT vendors and manages the procurement of hardware, software, and services. They evaluate and select appropriate technology solutions, negotiate contracts, and ensure compliance with licensing agreements and procurement policies.
- ix. **Project Management:** The directorate manages and coordinates ICT-related projects, such as infrastructure upgrades, system implementations, and software development initiatives. They follow

project management methodologies to ensure projects are delivered on time, within budget, and meet the defined objectives.

- x. **Collaboration and Partnerships:** The directorate collaborates with internal departments, academic units, and external partners to support research collaborations, technology transfer, and innovation initiatives. They engage in partnerships with industry, government agencies, and other educational institutions to leverage resources, share best practices, and stay abreast of technological advancements.

4.2.2 Centre for Digital Learning

The Center for Digital Learning (CDL) in the university is a dedicated unit that focuses on the development, implementation, and support of digital learning initiatives. Its primary goal is to leverage technology to enhance teaching and learning experiences, promote innovative pedagogical approaches, and support the integration of digital tools and resources into the curriculum. The Centre will be responsible for;

- i. **Online and Blended Learning:** The CDL facilitates the development and delivery of online and blended learning courses. It supports faculty in designing and developing engaging and interactive online courses that align with pedagogical best practices. The centre may provide instructional design expertise, multimedia production support, and learning management system (LMS) administration to enable effective online and blended learning experiences.
- ii. **Technology Integration:** The CDL promotes the effective integration of educational technology into teaching and learning practices. It offers training and support to faculty on using digital tools, learning platforms, and multimedia resources to enhance instruction and student engagement. The center stays abreast of emerging educational technologies and helps faculty explore innovative ways to incorporate them into the curriculum.
- iii. **School and Institute Development:** The CDL provides professional development opportunities for the institute and school members to enhance their digital teaching skills. This may include workshops,

seminars, webinars, and one-on-one consultations on topics such as online pedagogy, instructional design, assessment strategies, and accessibility considerations. The centre also fosters a community of practice where schools and institutes can share experiences and collaborate on digital learning initiatives.

- iv. **Learning Design and Course Development:** The CDL supports schools and institutes in designing and developing effective online and blended courses. This involves working with subject matter experts to create engaging learning materials, interactive multimedia content, and assessments that align with learning objectives. The centre may provide templates, guidelines, and resources for course design, ensuring consistency and quality across courses.
- v. **Learning Analytics and Assessment:** The CDL leverages learning analytics to collect and analyze data on student engagement, progress, and performance in online courses. This data helps faculty and instructional designers make informed decisions to improve course design, identify areas for intervention, and personalize learning experiences. The centre also assists in developing effective assessment strategies for online courses and provides support for rubric development, plagiarism detection, and feedback mechanisms.
- vi. **Student Support and Services:** The CDL offers support services to students participating in digital learning programs. This may include online orientation, technical support, access to online resources and tutorials, and guidances on effective online learning strategies. The centre collaborates with other student support services to ensure that students have a positive and successful learning experience in digital environments.
- vii. **Quality Assurance and Standards:** The CDL in collaboration with SUZA's Quality Assurance Unit (QA), shall establish quality assurance measures and standards for digital learning programs. It ensures that online courses meet established criteria for content quality, instructional design, accessibility, and student engagement. The centre may conduct course reviews, provide feedback and recommendations

for improvement, and facilitate the sharing of best practices among institute and school members.

- viii. Collaboration and Partnerships: The CDL collaborates with academic departments, faculty, and other university units to support interdisciplinary digital learning initiatives. It may partner with external organizations, industry partners, or other educational institutions to explore joint programs, share resources, and foster collaborations in the field of digital learning.
- ix. Evaluation and Continuous Improvement: The CDL evaluates the effectiveness of digital learning initiatives and programs and incorporates feedback from institutes, schools, and students to drive continuous improvement. It monitors and assesses the impact of digital learning interventions.

4.2.3 ICT Units in Schools and Institutes

Within university schools and institutes, ICT subunits play a crucial role in supporting the specific technology needs of their respective academic areas. These subunits, often housed within larger ICT departments, are dedicated to providing specialized services, support, and resources tailored to the requirements of specific schools or institutes.

4.2.4 The Governance Committee

To oversee the implementation of the policy's governance process, the following committees will be established and operational.

- 1) The ICT and Instructional Technology Committee
- 2) The ICT Technical Subcommittee (According to eGAZ/EXT/IGG/001)

4.2.4.1 The ICT and Instructional Technology Committee

The ICT and Instructional Technology Committee shall determine the overall functions and direction of ICT adoption in SUZA. The ICT and Instructional Technology Committee also shall concern with the improvement of the ICT policy and endorse guidelines under the ICT Technical Committee and ICT Services committee. The ICT and Instructional Technology Committee is the

decision making organ for all ICT related issues in the University whereby the critical issues are sent to the Council for approval.

The Council delegates the issue of ICT governance to the ICT and Instructional Technology Committee. The Committee is chaired by the Vice Chancellor. The Head of Centre for ICT services and the Head of Instruction Technology serve as the secretary of the Committee. The committee shall meet twice a year.

4.2.4.2.1 Members of the ICT and Instructional Technology Committee

- a) Representative from Council – Chairman
- a) Representative from Council - Member
- b) Vice Chancellor - Member
- c) Deputy Vice Chancellor - PFA - Member
- d) Deputy Vice Chancellor - ARC - Member
- e) Director of of ICT Services - Joint Secretary
- f) Head of CDL - Joint Secretary

4.2.4.2.2 Functions of ICT and Instructional Technology Committee

The ICT and Instructional Technology Committee will have the following functions:

- a) To oversee the overall direction of ICT at the University
- b) To receive and consider for approval inputs from ICT Technical Committee
- c) To approve ICT annual plans and quarterly performance reports of the Center of ICT Services
- d) To oversee ICT policy implementation and endorse the University ICT policy and Guidelines
- e) To develop and review ICT issues in SUZA Strategic Plan,
- f) To advise the university on effective use of technology for university development, and to improve teaching and learning functions.

4.2.4.2 The ICT Technical Subcommittee

There shall be an ICT Technical Subcommittee to oversee and advise the ICT and Instructional Technology Committee on ICT strategy and tactics developments and their use in the university.

The technical ICT subcommittee shall be responsible for defining and implementing the ICT policies at the university. This includes all ICT matters constituting its infrastructure, services, innovation, research, and development. To fulfill the university ICT needs, the technical ICT subcommittee shall execute its function in collaboration with the DICTS, CDL and SCCM. The committee shall meet on a quarterly basis.

4.2.4.2.3 Members of the ICT Technical Subcommittee

- a) DVC-ARC - Chairperson
- b) Director of ICT – Secretary
- c) Head of CDL - Member
- d) Head of departments of Computer Science and IT - Member
- e) Head of Unit of Media from SCCM - Member
- f) One internal ICT expert, appointed by the VC from the recommended list prepared by the Chairman of the ICTITC.

4.2.4.2.4 Functions of Technical ICT Sub-Committee

The functions of the ICT Technical Committee are:

- a) To review and advise on ICT policies, ICT strategic plan, operational procedures, ICT projects, and proposals.
- b) To support, develop, and enforce ICT standards, policies, and procedures at the SUZA.
- c) To promote harmonisation of ICT developments and activities engaged by schools, directorates, centers, departments, and individuals.
- d) To identify and promote areas of collaboration with other educational institutions in improving the use of ICT for university development.
- e) To receive and discuss ICT matters arising from schools and directorates.

- f) To set guidelines and review corporate ICT plans from schools, directorates, and centres.
- g) To advise the corporate planning process on strategic planning issues relating to ICT within the University.
- h) To advise on physical and environmental security maintained to protect University assets.

4.3 Legal and Regulatory Framework

The implementation of this policy will depend on the compliance of the following;

1. National ICT Guidelines and Regulations
2. University ICT Guidelines, Procedures and other Specific Policy (i.e. IP Policy)

All users of this policy will remain subject to the university's set of laws, regulations, and policies that govern the use of information and communication technology (ICT) within the university's environment.

4.4 Roles and Responsibilities of other Actors

The State University of Zanzibar is the owner of this policy, the contribution of other organs or departments in the implementation of this policy is also recognized. The successful implementation of this policy depends on the participation and cooperation of all university stakeholders.

4.4.1 The University Council

As the main governing body of the University, the Council will have the following roles:

- a) Review and approve ICT policy and provide strategic directives on the utilisation of ICT in order to enhance productivity by ensuring effective and efficient systems;
- b) Ensure implementation of the ICT Policy.

4.4.2 Deans and Directors

Deans and Directors are responsible for leading the integration of ICT within their schools and directorates, fostering collaboration to enhance teaching, learning, and research. In the implementation of this Policy, the Deans and Directors will have the following roles:

- a) Enforce the use of ICT within schools and directorates.
- b) Coordinate with the CDL to enhance the usage of ICT in teaching,
- c) Learning and research through the implementation of ICT initiatives.
- d) Initiate ICT initiatives and innovation within their schools and directorates

4.4.3 Departments, Centres and Units

Departments, Centres, and Units have a key role in enforcing the use of ICT within their areas and creating a conducive environment to foster ICT innovation and initiatives, as follows:

- a) Enforce the use of ICT within their departments/centres/units.
- b) Coordinate with the CDL on how to enhance the use of ICT in teaching, learning and research through the implementation of ICT initiatives.
- c) Create, manage and organise a conducive environment for ICT in initiatives and innovation within their departments.
- d) Advice on the effective ways of improving day to day activities with the integration of ICT

4.4.4 Users of ICT Systems

These are the main beneficiaries of the ICT services in the university. To ensure the smooth implementation of the policy, all users of ICT systems shall have the following roles:

- a) Shall be responsible for safeguarding all ICT assets of SUZA in their custody
- b) Shall comply with this policy and other guidelines

4.4.5 Internal Audit Unit

The Internal Audit Unit is responsible for evaluating and ensuring the effectiveness of the University's internal controls, risk management processes, and compliance with established policies and regulations. In the context of the ICT policy, the unit's role is to conduct regular audits of the ICT function at SUZA, ensuring that the policy is being adhered to and identifying areas for improvement in its implementation.

4.5 Monitoring and Evaluation

Monitoring and evaluation of a university ICT policy is crucial to ensuring its effectiveness, compliance, and continuous improvement. Implementation of the SUZA ICT Policy depends upon effective Monitoring and Evaluation (M&E) mechanisms to assess the implementation of strategies and achievement of policy goals and objectives. The policy will be reviewed every three (3) years to accommodate the emerging changes and monitoring and evaluation of this policy will be done in accordance to;

- i. **Policy Implementation Review:** Regularly review the implementation of the ICT policy to assess whether it is being followed effectively across the university. This entails assessing the comprehension of the policy by users, the adequacy of procedures and controls, and pinpointing any deficiencies or obstacles in implementation.
- ii. **Compliance Audits:** Conduct periodic audits to verify compliance with the ICT policy. This can include reviewing user activities, system logs, and data handling practices to identify any non-compliance or policy violations. Audits may be conducted by either internal audit teams or external experts.
- iii. **Incident Monitoring:** Monitor and track ICT-related incidents, such as security breaches, data breaches, or policy violations. Establish incident reporting mechanisms to capture and analyze incidents, enabling the identification of trends, vulnerabilities, and areas requiring policy adjustments.

- iv. **User Feedback and Surveys:** Gather feedback from users, including students, departments, centers, and staff, regarding their experience with the ICT policy. Surveys, feedback forms, or focus groups can provide valuable insights into the usability, effectiveness, and awareness of the policy. Identify areas for improvement based on user feedback.
- v. **Key Performance Indicators (KPIs):** Define specific KPIs aligned with the objectives of the ICT policy. These metrics could include measures such as the number of security incidents, compliance rates, user satisfaction scores, and response times for resolving policy-related issues. Regularly track and evaluate these KPIs to gauge policy performance.
- vi. **External Regulatory Compliance:** Monitor changes in relevant laws, regulations, and industry standards related to ICT and ensure that the university's ICT policy remains up to date and compliant with these external requirements. This may involve periodic reviews by legal experts or engagement with regulatory bodies.
- vii. **Stakeholder Engagement:** Engage with key stakeholders, such as IT departments, legal advisors, academic staff, student representatives, and administrators, to obtain their input on the ICT policy. Regularly communicate updates, changes, and clarifications to ensure stakeholders remain informed and engaged.
- viii. **Policy Review and Revision:** Schedule periodic reviews of the ICT policy to assess its relevance, effectiveness, and alignment with the evolving needs and technological advancements within the university. Solicit feedback from relevant stakeholders during these reviews and update the policy accordingly.
- ix. **Training and Awareness Programs:** Continuously assess the effectiveness of training and awareness programs related to the ICT policy. Monitor participation rates, evaluate the understanding of policy requirements among users, and gather feedback to improve training materials and methods.
- x. **Continuous Improvement:** Use the findings from monitoring and evaluation activities to drive continuous improvement of the ICT policy.

Identify areas for enhancement, address gaps or weaknesses, and update the policy as needed to ensure it remains current, effective, and aligned with the evolving ICT landscape.

4.6 Risk Management

Risk management plays a vital role in the implementation of university ICT policy. It involves identifying potential risks, assessing their potential impact, and implementing strategies to mitigate or manage those risks. The following methodology will be implied.

- a. Risk Identification: Identify the risks associated with the use of ICT within the university. This includes risks such as unauthorized access to sensitive data, data breaches, malware attacks, system failures, intellectual property theft, compliance violations, and reputational damage.
- b. Risk Assessment: Assess the potential impact and likelihood of each identified risk. Evaluate the severity of potential consequences, such as financial loss, disruption of services, compromised data integrity, legal penalties, or damage to the university's reputation.
- c. Risk Mitigation Strategies: the directorate will develop strategies to mitigate or manage identified risks. This can include a combination of technical controls, procedures, and employee training. For example, implementing strong access controls, encryption mechanisms, and firewalls can help reduce the risk of unauthorized access and data breaches. Regular data backups, disaster recovery plans, and incident response procedures can mitigate the impact of system failures or security incidents.
- d. Guideline Development and Communication: several guidelines will be in place as this policy direct that will clearly define the responsibilities, expectations, and guidelines for users to minimize risks. Ensure that the policy covers areas such as acceptable use, data protection, incident reporting, cybersecurity awareness, and compliance with relevant regulations. Communicate the policy effectively to all stakeholders and

provide training and awareness programs to ensure understanding and adherence.

- e. Incident Response and Business Continuity: The directorate will establish an incident response plan to effectively handle and mitigate the impact of security incidents, data breaches, or system failures. Define roles and responsibilities, escalation procedures, and communication protocols. The development of a business continuity plan will ensure minimal disruption to essential ICT services in the event of a significant incident.
- f. Continuous Monitoring and Review: Regularly monitor and review the effectiveness of risk mitigation measures, and the overall ICT policy will be the focus. Implement mechanisms to detect and respond to emerging risks and vulnerabilities. Conduct periodic security assessments, penetration testing, and vulnerability scanning to identify potential weaknesses and address them proactively.
- g. Compliance and Regulatory Requirements: This policy will ensure compliance with applicable laws, regulations, and industry standards related to ICT security and privacy.
- h. Risk Reporting and Documentation: The Directorate will maintain proper documentation of risk assessments, risk mitigation strategies, incident response plans, and compliance efforts. Develop reporting mechanisms to communicate risk-related information to relevant stakeholders, such as senior management, the board of directors, and external auditors.