SOUTH EASTERN KENYA UNIVERSITY

INFORMATION COMMUNICATION AND TECHNOLOGY (ICT) POLICY

January 2020

VISION

To be a globally competitive centreof excellence in teaching, research, innovation andservice.

MISSION

To provide quality education through teaching, research, extension, innovation andentrepreneurship with emphasis on food security, health, engineering and natural resources management.

CORE VALUES

Professionalism

Innovation

Integrity

Freedom of thought

Teamwork

Respect for and conservation of the environment

Discipline and hard work

PHILOSOPHY

South Eastern Kenya University is transforming lives and improving the environment fromarid to green through innovative teaching, research and community service.

TABLE OF CONTENTS

VISION i

MISSION i

CORE VALUES i

PHILOSOPHY i

ABBREVIATIONS vi

1. DEFINITION OF TERMS vii

2. FORWARD ix

3. PREFACE x

PART I. GENERAL INTRODUCTION 1

1. Purpose 1

2. The Scope of the Policy 1

3. The Policy Objectives 1

4. Implementation of the policy 2

5. Organization of the Policy Guidelines 2

6. Legal Framework 3

PART II. USE OF ICT RESOURCES 4

7. University Information & Communication Technology Resources 4

8. Acceptable use of ICT resources 4

9. Unacceptable Use 4

10. User Privileges and Expiry 5

11. Penalties for Unacceptable Use 6

12. User Acceptance 6

PART III. ICT EQUIPMENT MAINTENANCE 7

13. Support Levels 7

14. Maintenance of Hardware 7

15. Privately owned computer equipment and peripherals 7

16. Donations/Sponsored Computer Systems and Peripherals 7
17. Tools and Equipment 8
18. Campus workshops 8
19. Preventive maintenance 8
20. Outsourced Service Agreement for Critical Equipment 8
21. Obsolescence of hardware 8
22. Warranty guidelines 9
23. Maintenance Agreements and Service Level Agreements (SLA) 9
PART IV. MANAGEMENT OF ICT EQUIPMENT 10
24. Requisition 10
25. Acquisition 10
26. ICT Equipment Asset Register 10
27. Allocation of ICT Equipment and Responsibility 10
28. Custody of Equipment 11
29. Security and Loss of Equipment 12
PART V. INFORMATION SECURITY 13
30. Principles of information security 13
31. Information Classification 13
32. Incident Handling 14
33. Responsibilities of Data owners 14
PART VI. ELECTRONIC MAIL (E-MAIL) 16
34. Registration of Email Service 16
35. Appropriate Use of SEKU E-mail Services 16
36. Computer Viruses 17
37. Penalties for Improper Use of Email Services 17
38. Email Privacy and Security 17
PART VII. USER ACCESS MANAGEMENT 19

39. New User Registration 19
40. Deletion of Terminated User Account 19
41. User Access Rights/Change Request 20
42. Assignment of General User Access Rights 20
43. Assignment of Network User Access Rights 21
44. Assignment of Systems Administrator Access Rights 21
45. Assignment of Application User Access Rights 21
46. Assignment of Database User Access Rights 21
47. Reviewing User Access and Permissions 22
48. Monitoring of Users and Administrator(s) activity 22
PART VIII. PASSWORD GUIDELINES 23
49. Password Management Guidelines 23
50. Deletion of Password 23
51. Standards for Password Protection 24
52. Standards for Application Development 24
53. Remote User Access 25
PART IX. INTERNET USE 26
54. Provision of Internet Services 26
55. Acceptable use of Internet Services 26
56. Unacceptable use of Internet Services 26
57. Procedures for Request(s) and Approval of Internet Services 27
58. Maintaining Corporate Image 27
PART X. ICT TRAINING 29
59. ICT Literacy 29
60. Mode of Training 29
61. Training needs and Curriculum Development 29
62. Acknowledgement of training 30

PART XI. DISASTER RECOVERY 31
63. Functional Teams and Responsibilities 31
(1) Damage Assessment Team 31
(2) Executive Team 31
(3) Restoration Team 31
(4) Operations Team 32
(5) Customer Support Team 33
(6) Salvage/Reclamation Team 33
(7) Disaster Response 35
(8) Testing Disaster Recovery Site 35
PART XII. ICT IN THE LIBRARY 37
64. Guidelines for the use of ICT and Electronic Resources in the Library 37
PART XIII. REVIEW OF POLICY 40
PART XIV. ANNEXTURES 41
APPENDIX I. 41
APPENDIX II 42
APPENDIX III 43

ABBREVIATIONS

DR: Disaster Recovery

HRD: Human Resource Department

CCTV: Closed Circuit Television

ICT: Information and Communication Technology

ISP: Internet Service Provider

LAN: Local Area Network

OPAC: Online Public Access Catalogue

SLA: Service Level Agreement

SOS: Standard Operating System

UPS: Uninterruptible Power Supply

VOIP: Voice over Internet Protocol

VPN: Virtual Private Network

WAN: Wide Area Network

1. DEFINITION OF TERMS

(1) **Assets:** All applications and technologies that are owned, procuredand/or managed.

(2) **Data Center:** An ICT facility where equipment including servers, network equipment, storage facilities are installed and operated to ensure they are protected from physical damage or tampering with anaim to ensure service availability.

(3) **Data:** This is information that has been translated into a form that isconvenient to transmit or process.

(4) **Director, ICT:** Refers to the Head of ICT or any other personappointed to head the Directorate of ICT.

(5) **ICT**: Refers to technologies that provide access to information through telecommunications. It primarily focuses on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication media.

(6) **ICT equipment:** Refers to any device that can process, store or communicate electronic information, including computers, multifunction devices, landline and mobile phones, digital cameras, electronic storage media and other radio devices.

(7) **ICT system equipment**: Refers to a subset of ICT equipment that is used to maintain an ICT system, including servers, communications network devices such as PABX, gateways and network infrastructure such as cabling and patch panels—this equipment is normally continuously operational.

(8) **ICT facility:** Refers to a building, a floor of a building or a designated space on the floor of a building used to house or process large quantities of data; for example, server and computer laboratory, datacenters, back up repositories, storage areas for ICT equipment, and communications and patch rooms.

(9) **ICT system:** Refers to a related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.

(10) **Network infrastructure**: Refers to the infrastructure used to carry information between workstations and servers or other network devices. For example: cabling, junction boxes, patch panels, fiber distribution panels and structured wiring enclosures.

(11) **University**Refers to South Eastern Kenya University.

(12) **E-mail**: Refers to messages distributed by electronic means from one computer user to one or more recipients via a network.

(13) **SEKU Data,** for the purposes of this policy, is data owned, processed or held by SEKU, whether primary or secondary, irrespective of storage location. It is used interchangeably with the term 'information'.

(14) **Administrative rights:** Access rights that allow a user to perform high level/administrative tasks on a device/application such as adding users, deleting log files, deleting users.

2. FORWARD

The University Council is committed toproviding an enabling environment for use of ICT resources in an effective, efficient and responsible manner so as to realisemaximum benefit from the facilities. South Eastern Kenya University (SEKU) aims to harnessing ICT to fully automate its processes and procedures to transform service delivery to its clients. This Policy will, among other things, aid the University in complying with the National ICT Policy (2014).

The University Council calls upon the entire University Community to familiarisethemselves with the objectives and provisions of this policy and to ensure compliance and implementation.

DrSwabah Omar

COUNCIL CHAIRPERSON

3. PREFACE

In its 2019-2023 Strategic Plan, the University has identified the development of ICT infrastructure to support teaching, learning, research, administration and outreach as a key strategic objective.The University has grown its ICT capacity in its journey towards becoming a world class university.

The University grants members of the University community shared access to the ICT resources as a way of accomplishing its mission and mandate, and recognises ICTas a vital facilitator to all faculty, staff and students.

The University has the responsibility of ensuring that ICT resources are used for the intended purpose.This ICT Policy, therefore, servesas a guidefor effective use of these resources. ThePolicy seeksto identify ICT services incorporated within the University ICT infrastructure and define a governance and management structure. It articulates the guidelines, framework andprogrammeof actions adopted by the University for the implementationand use of ICT. It describes critical areas for the development and application of ICT by laying out the blueprint in terms of the University's strategy on using ICT as an enabling tool.

Prof. Geoffrey M. Muluvi PhD.

VICE-CHANCELLOR

PART I. GENERAL INTRODUCTION

1. Purpose

The purpose of this Policy is to give a guideline to the South Eastern Kenya University (SEKU) community on the utilisationof information,communication technology (ICT) to enhance service delivery and promote compliance. It covers the best practices for ICT in the standardisationof processes that create economies of scale, permitting the University to deliver its core mandate with the available ICT resources. This covers the use of computers and other related hardware such as printers, projectors and network infrastructure.

Further, this Policy shall ensure availability, confidentiality, security, and integrity of ICT resources, which support the operations of the University.

2. Scope

(1) This policy applies to all SEKU staff and students or any other person(s) or organization(s) accessing services over University ICT resources; persons contracted to develop, repair or maintain the University's ICT resources and suppliers of outsourced ICT services.

(2) The ICT Policy defines and guides the University's use of ICT resources, software, systems, hardware devices, infrastructure, network systems, and any other ICT solutions. The Policy shall also apply to all equipment owned or leased by the University.

(3)

3. Objectives

(1) To define what constitutes acceptable use of the ICT resources of South Eastern Kenya University.

(2) To outlines the rules and guidelines that ensure that users' Computers and related hardware are in serviceable order.

(3) To provides a guideline for the management of all ICT resources from procurement to disposal by keeping an up-to-date and accurate database of all ICT resources.
(4) To provide guidelines that ensure availability, confidentiality, security, and integrity of the University's information systems and its assets from anythreats - internal or external, deliberate or accidental.
(5) To provide guidelines on the use of e-mail services provided by the University.
(6) To provide a guideline on the user access management controls for the University's ICT systems users both internal and external.
(7) To provide a standard guideline for the creation of strong passwords, protecting those passwords, and the frequency of change.
(8) To define an appropriate guideline for the uses of the Internet by the University's employees, students, and affiliates.
(9) To outline the guidelines that guide when planning for, organizing and conducting ICT training at the University.
(10) To provide a structured approach for responding to incidents thatthreaten the ICT investments.
(11) To provide a regulatory environment and framework for the application of ICTs in the delivery of library services.

4. Implementation

The Director, ICT is responsible for the day to day implementation of this Policy.

5. Organization of the Policy guidelines

The contents of this Policy are contained in ten chapters under the following headings: Use of ICT Resources, ICT Equipment Maintenance, Inventory of ICT Equipment, Information Security, Electronic Mail, User Access Management, Password Guidelines, Internet Use, ICT Training, Disaster Recovery and ICT in the Library.

6. Legal framework

This Policy subscribes to the Constitution of Kenya, 2010, Access to Information Act No. 31 of 2016, Computer Misuse and Cyber Crimes Act No. 5 of 2018 and all other relevant legislation of Kenya. The Policy is also compliant with Article 35 of the Constitution of Kenya which provides for the right of every person to information required for the protection of any right or fundamental freedom. This Policy therefore aims at ensuring that the rights of individuals in as far as ICT is concerned are safeguarded. The Policy is also guided by the National ICT Policy, National ICT Master Plan, The ICT Authority Standards and other University policy documents.

PART II. USE OF ICT RESOURCES

7. University Information andCommunication Technology resources

The ICT resources of SEKU include:

(1) Hardware

(2) Software

(3) Networking equipment, services and facilities

(4) Communication equipment, services and facilities

(5) Data and information owned, leased, or loaned, by SEKU or its agents.

8. Acceptable use of ICT resources

Acceptable use means an accountable, rational and appropriate exercise of a freedom to use while respecting the rights of other computer users, the integrity of the University's ICT resources and all pertinent licenses and contractual agreements.University information systems are to be used solely for University-related business, inclusive of teaching and learning processes. However, personal use of computers may be permitted if such use conforms to the general University regulations and do not interfere with University operations, degrade its goodwill or negatively impact intended learning outcomes of students or performance of duties by employees.

9. Unacceptable use

Use of SEKU's ICT resources is a privilege extended by the University to its staff, *bona-fide*students and otherrecognised parties. Any use of SEKUICT resources will be considered unacceptable if it:

(1) conflicts with its aims and objectives;

(2) breaches any of its statutesor ordinances;

(3) violates national laws;

(4) intentionally circumventsor compromiesthe security controls or integrity of the University ICT resources or any other computer or communication network resource connected to it;

(5) intentionally denies access to or interferswith any network resources;

(6) usesor accessesany University ICT resource information or data, without proper authorization;

(7) usesthe University ICT resources to attack computers, accounts, or other users by launching viruses, worms, Trojan horses, or other attacks on computers in the University or elsewhere;

(8) conductscommercial activity not duly approved by the University;

(9) usesthe University's ICT resources to misrepresent or impersonate someone else; or

(10) usesthe University's ICT resources for any purpose which the University deems obscene or offensive.

10. User privileges and expiry

(1) SEKU shall implementguidelines that define access to computing and communications resources to all system users. The University reserves the right to withdraw such privileges, pursuant to contract stipulations as well as actions speltout in *Part II (3)*of this Policy.

(2) The following list maps basic user privileges and expiry of those privileges.

(a) Full-time, part-time and contract staff

(i) University desktop PC with approved software suite.

(ii) User account for SEKU electronic mail and web browsing.

(iii) Access to shared work server and main shared applications server.

(iv) VPN access to above services where applicable.

(v) The expiry date of the above shall be the separation date.

(b) Students

(i) User account(s) for SEKU electronic mail and web browsing.

(ii) Access to University computer laboratories.

(iii) The expiry date shall be the termination date of studentship.

(b) Intern

(i) University based desktop PC with approved software suite.

(ii) User account for SEKU web browsing.

(iii) The expiry date shall be the official end date of internship.

(c) Supplier/business partner

(i) Web browsing account.

(ii) User access account to University resource or service they are working on.

(iii) The expiry date shall be the date of termination of partnership or contract.

(3) The Director ICT, in liaison with the Human Resources Department, shall approve any additional privileges, or extension of expiry dates. The Director ICT shallensure all expiries are enforced.

11. Penalties for unacceptable use

Where there is evidence of unacceptable use, the University may:

(1) restrict or prohibit the use of its ICT resources;

(2) revoke access to University systems and ICT services;

(3) institute disciplinary action in accordance with the University policy;

(4) initiatecivil or criminal proceedings.

12. User acceptance

All users of the ICT resources of SEKU shall abide by theseguidelines and shall signify acceptance of the same.

PART III. ICT EQUIPMENT MAINTENANCE

13. Support levels

The University shall implement four (4) levels of support to users of ICT equipment.

(1) ***First Level Support:***Reported basic issues can be resolved on phone.If issues are not resolved at this level, they shall be escalated to the Second Level Support.

(2) ***Second Level Support:***An ICT staff shall offer support to the users.

(3) ***Third Level Support:*** An ICT specialist shall handle unresolved issues.

(4) ***Fourth Level Support:*** The Directorate of ICT shallwork in liaison with vendors, suppliers and hardware manufacturers to resolve the issue.

14. Maintenance of hardware

The Directorate of ICT shall maintain and support the hardware equipment commonly used in offices, computer rooms, laboratories and lecture theatres.

15. Privately owned computer equipment and peripherals

The University maypermit users to connect to its network using privately owned computers. However, the Directorate of ICT shall not take responsibility for the loss, replacement, repair or upgrade of privately owned equipment or peripherals.

16. Donations or Sponsored Computer Systems and Peripherals

(1) Donated computers and related accessories shall become University property and shall be maintained by the Directorate of ICT.

(2) The Directorate shall ensure the following:

  (a) Satisfactory operating environment (floor space, climate control, ventilation, and backup power supply) for the system.

  (b) Installation and administration of the system.

(c) Routine maintenance and upgrade of the system.
(d) Full compliance with the University's Procurement and Disposal Policy/Act.
(e) Full compliance with the University's security policy, including installation and regular update of the anti-virus software.
(f) Supplyofspares to support such systems and peripherals.

17. Tools and Equipment

Every campus shall have ICT personnel well equipped with ICT support tools and equipment.

18. Campus workshops

Every campus shall have a designated repair facility. The ICT personnel in suchcampus shall have custody of such facility.

19. Preventive maintenance

A schedule for maintenance shall be drawn, recognisingevery piece of hardware. Preventive maintenance shall be carried out according to the recommendations of the manufacturer of the hardware. However, unscheduled maintenance may be considered depending on the circumstances.

20. Outsourced service agreement for critical equipment

Equipment not supportable by the Directorate of ICT shall be placed on maintenance contracts with the appropriate vendor.

21. Obsolescence of hardware

(1) ICT hardware shall be declared obsolete if:

(a) the hardware has served the recommended life span according to the recommendations of the manufacturer;

(b) The hardware is declared irreparable by the Directorateof ICT and the same is confirmed by the assets disposal committee in accordance with the Procurementand Asset Disposal Act (2015) and related regulations.

22. Warranty guidelines

(1) The ICT staff shall ensure that equipment under warranty isrepaired and maintained according to the manufacturer's warranty agreement document.

(2) The staff shall keep accurate records of the warranty and use such information when needed.

23. Maintenance Agreements and Service Level Agreements (SLA)

The DirectorICT shall be charged with the responsibility of enforcing any maintenance contracts, agreements and warranties.

PART IV. MANAGEMENT OF ICT EQUIPMENT

24. Requisition

Requisition for all ICT equipment and accessories shall be made by the respective Headsof Sections, Registrars or Directors to the Director ICT. The Director ICT shall on a regular basis consolidate such requisitions and prepare technical specifications and requirements.

25. Acquisition

(1) ICT equipment can be acquired through purchase or donations.
(2) Purchase of ICT Equipment shall be guided by Government procurement regulations. All goods shall be received and inspected at the Procurement Department for compliance before distribution to the end user.
(3) Donated equipment shall be received and inspected for performance, compliance and conformity.

26. ICT equipment assetsregister

(1) The Directorate of ICT shall maintain an ICT asset register. This register shall monitor procured ICT equipment issuance, usage, surrender, movement, maintenance and loss. The register shall contain details and particulars of ICT equipment.
(2) All ICT equipment shall be tagged with a unique identification code that shall be part of the assetsregister details.
(3) ICT staffshall conduct quarterly inventory audit of ICT equipment and submit a report to the Director ICT to update the assets register.
(4) University ICT equipment in functional units that are no longer in use shall be surrendered to the Directorate of ICT.

27. Allocation of ICT equipmentand responsibility

(1) ICT equipment shall be allocated to individual employees as per the criteria on ICT equipment allocation and entitlement.

(2) Employees with requests for new equipment shall submit their requestswith a written justification to the Vice-Chancellor through the Director ICT.

(3) The Director ICT shall ensure that ICT equipment in the University is standardisedto optimisemaintenance costs.

(4) Should any employee or user require specialisedequipment other than what the University provides, such employee or usershall submit a request in writing to the Vive-Chancellor through the Director ICT.

(5) The procurement and issuance of ICT equipment shall comply with the relevant University policies and regulations, and the Procurement and Disposal Act (2015).

(6) Officers issued with new or replacement equipment shall surrender the old equipment upon receipt of the new or replacement equipment. ICT Officers together with the users shall ensure that data is transferred to the new equipment.

(7) All officers shall ensure they sign the equipment issueform and retain a copy thereof. In case of anomalies, the records held by the University shall prevail.

(8) All users and employees shall be responsible for equipment issued to them and shalltreat them with care.

(9) All shared ICT equipment such as printers, scanners and telephone extensions allocated to offices or work stations and functional units shall be the responsibility of the respective Heads of the stations or units.

(10) Non-employees of the University shall only be issued with ICT equipment upon written approval from the Vice-Chancellor.

28. Custody of equipment

(1) The management of ICT equipment shall be done in collaboration with the Procurement unit and all requisition, allocation and /or movement of equipment shall be in line with existing procurement laws and regulations.

(2) All users and employees issued with laptops and other mobile devices for use within or outside the University premises shall be responsible for the safety and care of the same.

(3) All University employees issued with laptops, tablets and/or mobile devices, upon transfer shall move with them to their new work stations and must fill and submit ICT asset movement form (Refer to Appendix III).

(4) Any other ICT equipment,including desktop computers and printers, shall not be moved from the current station.

(5) ICT equipment shall not be relocated from one office to another without filling and submitting the ICT assetsmovement form to the Director ICT for prior approval.

(6) All employees issued with ICT equipment shall surrender them beforeexit from the service of the University.

29. Security and loss of equipment

(1) Security of ICT equipment shall be the responsibility of the user. Loss of equipment must be reported to the Head of Security immediately. Replacement for the lost equipment shall require written approval from the Vice-chancellor.

(2) Necessary precaution shall be taken while using ICT equipment out of the University premises. Failure to demonstrate due diligence in protecting equipment shall constitute negligence and the user shall be held liable for the loss.

(3) All employees must be cognizant that the loss of data held in any ICT equipment exposes the University to serious security lapses. Necessary measures (technical and procedural) should be taken to protect the data in the devices.

PART V. INFORMATION SECURITY

30. Principles of information security

(1) Information shall be classified based on appropriate level of confidentiality, integrity and availability, and in accordance with relevant legislative, regulatory and contractual requirements and this Policy.

(2) Staff with particular responsibilities shall be responsible for handling such information according to its classification (PART V (3)).

(3) Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.

(4) Information will be protected against unauthorisedaccess orprocessing in accordance with its classification level.

(5) Breachofthese guidelinesshall be reported to the Director ICT (PART V (4)).

31. Information Classification

(1) The following isa summary of the information classification levels that have been adopted by the Universityand which underpin the eightprinciples of information security defined in theseguidelines.

(2) These classification levels explicitly incorporate the Data Protection Act(2012) definitions of *personal data*and *sensitive personal data*designed to cover both primary and secondary research data.

(a) Confidential data

Confidential information is accessible only to specified members of SEKU.These include sensitive personal data used as primary or secondary research data, bank details and passwords.

(b) Restricted data

These are data accessible only to specified members of SEKU staff or the student body.They include information that identifies living individuals including home

orwork address, age, telephone number, University attended, photographs;committee business; draft reports, papers and minutes; systems.

(c) Internal use.

Dara or information that are normally accessible only to members of SEKU staff and the student body. These may include: internal correspondence, final working group papers and minutes, committee papers, information held under license

(d) Public

Data that areaccessible to all members of the public. Theseinclude information available on the University's website or through the University'spublications.

32. Incident Handling

Any information security incident shall be reported to the Director ICT or the Directorate of ICThelpdesk. To report via email, use icthelpdesk@seku.ac.ke.

33. Responsibilities of data owners

(1) Members of SEKU and other stakeholders willbe users of SEKU information, and shall abide by the guidelines, principles, relevant legislation, supporting policies and procedures. No individual may access information to which they do not have a legitimate access right.

(2) Data Owners: Members of SEKU will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

(a) Principal Project administrators: Responsible for the security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities.

(b) Directors/ Deans/Heads of Departments, Divisions, and Sections: Responsible for the information systems both manual and electronic that support SEKU's work.

(c) Head of Department: Responsible for specific area of SEKU work, including all the supporting information and documentation that may include working documents/contracts/staff or student information.

(d) Director of Research Innovations and Technology: Keeps a record of all SEKU research contracts.

(e) ICT Staff: Responsible for ensuring that the provision of SEKU's ICT infrastructure is consistent with the demands of this guidelines and current good practice.

(f) Head of Security: Responsible for providing specialist advice on physical of security matters.

(g) Director, ICT: Responsible for information security guidelines and shall provide specialist advice to the University on information security issues.

PART VI. ELECTRONIC MAIL (E-MAIL)

34. Registration of e-mail service

(1) All staff and students shall be provided with a unique e-mail accountto facilitate the day to day University and the administrativefunctions. An e-mail request form shall be completed by the user.

(2) The e-mail address shall include the first name and an alternate.

(3) The University e-mail service shall not be used for unlawfulactivities, commercial purposes, personal financial gain orother usesinconsistent with the University policies.

35. Appropriate use of SEKU e-mail services

(1) All staff and students of SEKU shall have a corporate e-mail account for official use.

(2) Users may not use SEKU email services and/or facilities, to transmit:

(a) examination papers intended for an examination session prior to the writing of the examination;

(b) examinations results;

(c) commercial material unrelated to the legitimate business of SEKU, including the transmission of bulk e-mail advertising;

(d) bulk non-commercial emails not relevant to users;

(e) unsolicited e-mail messages requesting other users to continue forwarding the same e-mail (electronic chain letters);

(f) e-mail messages which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing);

(g) material which is offensive or inappropriate;

(h) material that incites criminal activity, or thatmay otherwise damage SEKU's image;

(i) material to which a third party holds an intellectual property right, without the express written permission of the right holder;

(j) material that is defamatory, libelous, harassing, threatening, discriminatory or illegal;material that could be used to breach computer security, or facilitate unauthorisedentry into computer systems;

(k) material that is likely to prejudice or seriously impede the course of justice in Kenya in terms of criminal or civil proceedings;

(l) messages that could imply the creation of an order or contract contrary to SEKU's Financial Regulations.

(3) Caution should be exercised when drafting e-mail which references personal data. Encryption may be used to ensure confidentiality.

(4) Incidental and occasional personal use of e-mail shall be permitted so long as such use does not disrupt SEKU business.

(5) Users shall not knowingly allow use of their accounts by people other than themselves. Users will be deemed liable for any e-mail or activity from their accounts.

36. Computer viruses

(1) Steps shall be taken to prevent the propagation of computer viruses throughe-mail. All computer systems shall have updated anti-virus software installed.

37. Penalties for improper use of e-mail services

Failure to comply with the guidelines on use ofe-mail services may result in withdrawal of access, disciplinary action, civil action, and prosecution.

38. Email privacy and security

(1) The following steps shall be taken to minimisethe risk of interception or breaches of confidentiality:

(a) Non-disclosureofuser passwords to unauthorised persons.

(b) Not allowing other users to send e-mail from your account

(c) Ensuring that the correct recipient e-mail address is used.

(d) Confirming the identity of an e-mail sender in case of doubt.

(e) Adopting a risk-based approach to deciding what information is appropriate to be sent by e-mail.

(2) The use of e-mail disclaimers is discouraged.

(3) A deleted e-mail message by both sender and receiver exists and in their systems. The University shall uphold the Kenyan Laws on Retention of electronic records as stipulated in the *Kenya Information and Communications Act, 1998. [CAP. 411A]*.

(4) Users shall not, under any circumstances, monitor, intercept or browse other users' e-mail messages.

(5) SEKU reserves the right to inspect, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse.

(6) SEKU reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes.

(7) SEKU reserves the right to demand that encryption keys, where used, be made available so that it is able to fulfil its right of access to a user's e-mail messages in such circumstances.

(8) Any personal organizer, holding mail messages, e-mail addresses (or any other confidential material) shall be password protected.

PART VII. USER ACCESS MANAGEMENT

39. New User Registration

(1) A formaliseduser registration process shall be implemented and followed in order to assign access rights.

(2) All user access requests shall be formally documented, along with the access requirements, and approved by authorised personsupon the completionof the user access request form (SeeAppendix II).

(3) User access requests formsshall be obtained from the Directorate of ICT or downloaded from the University website under ICT downloads.

(4) The duly completedform shall be forwarded to the Head of Section for access requirements to be approved.

(5) Once the requirements have been requested and endorsed by the SectionHead, the form shall be sent to the Director of ICT for approval and activation of the user account.

(6) User access rights shall only be granted once approval has been obtained.

(7) All users shall be assigned unique user IDs in order to ensure accountability for actions performed.

40. Deletion of terminated user account

(1) A formaliseduser termination process shall be followed in order to revoke access rights.

(2) All user termination requests shall be formally documented and approved by the Deputy Vice-Chancellor - AHRM.

(3) Account access shall be disabled immediately, with accounts being deleted after sevenyears.

(a) Terminated user requests shall be obtained from HR on the termination of an employee. The template for this type of request is attached to this Policy in Annexure B. The form shall be sent to the service provider or line manager for access revocation to be endorsed. Once access revocation has been endorsed, the form shall be sent to the Directorate of ICT for approval and deactivation of employee based on specified requirements.

41. User access rights/change request

(1) A formaliseduser access management process shall be implemented and followed in order to adjust user access rights.
(2) All user access change requests shall be formally documented, along with their access requirements, and approved by the duly authorised persons.
(3) Access shall only be granted once approval has been obtained by the head of section (**Appendix II)**.
(4) The form shall be sent to the Head of Section for access requirements to be endorsed.
(5) Once the access requirements have been endorsed, the form shall be sent to the Director ICT for approval and adjustment of employee's access rights based on specified requirements.
(6) User access change requests shall be obtained from respective Head of Section on change of an employee's role or permissions (**Appendix II)**.
(7) User access rights that are no longer required shall be removed immediately.

42. Assignment of general user Access rights

(1) Access rights include, but are not limited to:
    (a) General office applications (E-mail, Microsoft Office, SharePoint.).
    (b) Department specific applications and/or databases.
    (c) Network shares.
    (d) Administrative tasks.
    (e) RAS/VPN access.
    (f) Wi-Fi.
(2) Access shall follow a "principle of least-privilege" approach, whereby all access is revoked by default and users are only allowed access based on their specificrequirements.
(3) The levels or degrees of access control to classified information shall be restricted in terms of legislative prescripts.

(4) Access rights shall be assigned to a group/role and a user shall be assigned to that group.
(5) Access rights shall not be assigned to individual users.

43. Assignment of network user access rights

(1) Access to the University's network shall only be allowed once a formal user registration process has been followed.
(2) Access to Wi-Fi shall only be provided to users who require access to the network throughout the University to fulfil their duties.

44. Assignment ofsystems administrator access rights

(1) System Administrator(s)shall be given a personalaccount with the administrator privileges.
(2) Should need arise for a shared account(s) to fulfil a business function, this account shall be approved and documented by the Director, ICT.
(3) The default administrator account shallalways be renamed, the password shall be randomly generated and documented by the Director, ICT.
(4) The default guest account shall be removed or renamed and disabled.

45. Assignment of Application User Access Rights

(1) Segregation of duties shall be practiced in such a way that application administrators cannot perform general user tasks on an application so as to prevent any fraudulent activity.
(2) Without any exceptions, Applications administrators shall remain independent of the department utilisingthe application.

46. Assignment of database user access rights

(1) The Director, ICT,shall limit full access to databases.
(2) The system administrators,who need this access,shall be granted rights based on their roles.
(3) University employees who use applications shall not have rights to the application's databases.
(4) The Director, ICT, shall review database rights and permissions on a bi-annualbasis or need arises, and remove excessive rights and permissions.

47. Reviewing User Access and Permissions

(1) User access and user permissions shall be reviewed every three months by system administrators.
(2) All terminated employees' systems accounts shall be revoked immediately upon receiving a copy of the termination letter from the DVC-AHRM.
(3) On a monthly basis, the Director, ICT,shall review all users with administrative access to the environment and assess their rights for appropriateness.
(4) All reviews shall be formally documented and signed by the Director, ICT.

48. Monitoring of Users and Administrator(s) activity

(1) User and administrator activity shall be monitored through audit and event logging.
(2) The system administrators and application owners shall review audit and event logs for suspicious and malicious activities on a monthly basis or asneed arises.
(3) Dormant accounts shall be disabled and a request to remove the access should be made.
(4) All reviews shall be formally documented for records purposes.

PART VIII. PASSWORD GUIDELINES

49. Password management guidelines

(1) Password construction requirementsshall satisfy the following criteriaon all systems:

(a) A minimum length of eight (8) characters.

(b) Not a dictionary word or proper name.

(c) Not the same as the user ID.

(d) Should expire within a maximum of 90 calendar days.

(e) Should not be identical to the previous 10 passwords.

(f) Should not be transmitted in the clear or plaintext outside the secure location.

(g) Should not be displayed when entered.

(h) Should only be reset for authoriseduser.

(2) These password requirements shall be enforced by any ERP or System in use or acquired by the University at the time of password creation for accounts issued.

(3) Employees shall ensure that they change the issued e-mail or system password on the first login.

(4) Employees shall be required to change their password at least two (2) times a year to enhance security of the email or system account(s).

50. Deletion ofpassword

(1) All passwords that are no longer needed shall be deleted or disabled immediately. This includes, but is not limited to, the following:

(a) When a user retires, dies, quits, is reassigned, released,dismissed.

(b) Default passwords shall be changed immediately on all equipment after the first logon.

(c) Contractor accounts, when no longer needed to perform their duties.

(2) When a password is no longer needed, the following procedures shall be followed:

(a) The Head of Section shall notify the Director, ICT, to deactivate user account.

(b) If the user is a contractor, the point-of-contact (POC) shall inform the Director ICT to deactivate the user account.

(c) The Supervisor or POC shall communicate in writing, requesting for password deletion.

(d) The Director, ICT,shalldelete the user's password or suspend the user's account.

(e) The systems administrator shall ensure that the password has been deleted and user account deleted or suspended.

(f) The account suspension or password deletion requestshall be filed in a secure filing system.

51. Standards for password protection

(1) User ID shall not be used asa password.

(2) User passwords shall not be shared.

(3) All passwords shall be treated as sensitive and confidential.

(4) If an account or password is suspected to have been compromised, the incident shall be reported to the Director ICT.

(5) Authorisedpassword cracking or guessing may be performed on a periodic or random basis by the Director, ICT,and if a password is guessed or cracked during anyof these scans, the user shall be askedto change it.

52. Standards for Application Development

Application developers shall ensure their programmescontain the following security precautions:

(1) Support authentication of individual users, not groups.

(2) Donot store passwords in clear text or in any easily reversible form.

(3) Provide role management sothat one user can take over the function of another without having to know the other's password.

53. Remote useraccess

(1) Access to the SEKU networks via remote access shall be controlled by using either a Virtual Private Network or a form of advanced authentication (Biometrics, Tokens, Public Key Infrastructure, and Certificates among others).

PART IX. INTERNET USE

54. Provision of internet services

(1) The Directorate of ICT shall provide Internet access to allemployees and students. All University employees are expected to use theinternet responsibly as prescribed in PART IX (2).

(2) The University reserves the right to monitor internet usage forthe purposes of managing system performance, ensuring compliance with policies, or as part of security, disciplinaryor other investigations.

55. Acceptable use of Internet services

(1) Employees shall use the Internet responsibly as prescribed inthe acceptable user guidelines

(2) The use of the Internet is encouraged for related University business and purposes such as research, skills development,office activities andgeneraldevelopment of the University.

(3) The University shall provide Internet services for businessrelated communication and collaboration between staff, students and/or other entities.

56. Unacceptable use of Internet Services

(1) Employees shall not use the Internet for personal gain orpersonal business activities.

(2) Employees shall not use the Internet for disseminating orprinting copyrighted material in violation of copyright laws.

(3) Employees shall not use the Internetto carry out activities thatcould cause congestion and disruption of University networkand systems.

(4) Employees shall not use the Internet for inappropriate andunlawful content. Use of the Internet shall conform to theUniversity employees Code of Conducts.

57. Proceduresfor Request(s) and Approval of Internet Services

(1) Employees shall be required to read, understand and commit to adhere to these guidelines.
(2) Employees shall fill the Internet Usage Acknowledgment Form (Appendix I), approved by the supervisor and submit it to the Director, ICT.
(3) Internet services shall be provided to users via cable or wireless access points depending on the infrastructure in place in the different work areas.
(4) Internet access shall be discontinued upon separation.
(5) All users shall follow the corporate principles regarding resource usage and exercise good judgment in using the Internet.

58. Safeguarding SEKU's name and reputation

(1) **Representation**

When using University resources to access and use the Internet, users shallremain alive to the fact that they represent SEKU. Whenever employees state an affiliation to SEKU, they shall also clearly indicate that the opinionsexpressed are their own and not necessarily thoseof the University.

(2) **University materials**

Internet users shall not place University material on any mailing list, public news group, or such a serviceunlesssuch materials are approved by the Vice-Chancellor through the Public Relations Manager.

(3) **Creating of web sites**

(i) All individuals and business units wishing to establish a personal home page or site shall first develop business, implementation, and maintenance plans.
(ii) Formal authorisationshall be obtained through the Director, ICT, in order to maintain consistency and appropriate standard of publishing content.

(iii) Contents of the material made available to the public through the Internet shall be formally reviewed and approved before being published.

(iv) All material shall be submitted to the Public Relations Department for initial approval.

(v) All University pages are owned by, and are the ultimate responsibility of, the Public Relations Department.

(vi) All University web sites shall be protected from unwanted intrusion through formal security measures which can be obtained from the Director,ICT.

PART X. ICT TRAINING

59. ICT literacy

(1) It shall be mandatory for all employees to be literate users of ICT services, the level of literacy being in line with the demands of their job functions.
(2) ICT training shall focus on building skills in users, making them effective in exploiting provided ICT resources.

60. Mode of Training

(1) Internal ICT user training targeting the University community shall be scheduled on a continuous basis and shall be conducted in computer laboratoriesboth atthe Main Campus and the satellite campuses.
(2) External ICT training shall be organized by the Director,ICT,in response to need as may be assessed from time to time when training is not possible within the University.
(3) The Director,ICT, in liaison withthe user departments,shall nominate trainees for external ICT training.
(4) Campus directors shall nominate trainees jointly with the user departments every quarter and forward the list to the Directorate of ICT.
(5) The number of trainees shall be as per the Strategic Plan for the campus or unit.
(6) The Director,ICT, shall identify appropriate trainers for the training.
(7) The Director,ICT, shall provide the necessary resources to facilitate the training.

61. Training needs and curriculum development

(1) The Human Resource Department shall conduct annual ICT training needs assessment in the University to advise on ICT training requirements.
(2) The Directorate of ICT and developers shall establish ICT training needs in liaison with user departments and service consumers. In cases where the Directorate is not

well placed to train in a given area, the ICT Director shall identify and recommend appropriate training and work out the cost for competent trainers.

(3) The School of ICT shall develop a curricula for all training including development of source material. To this end, the ICT Director shall:

(a) recommend curriculafor all external training

(b) where possible, provide training materials on-line via the University website.

(c) where possible, conduct an online assessment tests and examinations.

(d) where external training is sourced, jointly with the external training agent, customisethe content to meet users'training needs.

62. Acknowledgement of training

(1) Every trainee shall sign an attendance register after every training session.

(2) The Directorate of ICT shall issue certificates on successful completion of training.

PART XI. DISASTER RECOVERY

63. Functional teams and responsibilities

This section describes each team's role and its responsibilities in preparing for and responding to a disaster.

(1) Damage assessment team

(a) This team assesses the damage level of the server room, estimates the duration of the outage and submits a report with recommendations to the Executive Team.

(b) Itsresponsibilities include:

(i) receivingthe first alert regarding the disaster;

(ii) coordinatingwith the security personnel and/or fire department to ensuring safety, security, and access to the damaged facility;

(iii) assessing the level of damage to the ICT infrastructure; and

(iv) reportingto the Executive Team with recommendations.

(2) Executive team

(a) The Executive team declares that a disaster has occurred, approves and oversees the execution of the ICT disaster recovery plan.

(b) Itsresponsibilities include:

(i) reviewing the assessment report;

(ii) declaringa state of disaster;

(iii) establishinga command and communicationscentre;

(iv) activatingthe functional team;

(v) notifyingthe Key Executives; and

(vi) monitoringthe performance of the disaster recovery teams andtheexecutionandeffectivenessofthedisaster recovery plan.

(3) Restoration team

(a) The restoration team brings the DR site to operational mode by managing the relocation of services, and also manages the relocation of services back to the server room.

(b) The pre-disaster responsibilities are to:

(i) establish and maintain the recovery procedures for the DR site;

(ii) manage and maintain the backup procedures;

(iii) establish and maintain the disaster recovery data communications link to the DR site; and

(iv) planand conduct regular DR site recovery tests.

(c) The disaster responsibilities and actions are:

(i) coordinatingrecovery procedures'

(ii) restoringthe operating systems environments on the DR site host systems;

(iii) establishingthe data communications link to the DR site;

(iv) verifyingthat the operating systems and all other system and communication software are working properly;

(v) supportingthe operations at the DR site by resolving problems and monitoring and maintaining the data communications link to the DR site.; and

(vi) coordinatingthe return of operations to the server room.

(4) Operations team

(a) The operations team assists in the recovery operations and manages the operations of the computer systems at the DR site.

(b) The pre-disaster responsibilities is to maintain current and up-to-date systems operations documentation.

(c) The disaster responsibilities and actions are to:

(i) provide assistance to the Restoration Team in the restoration of the systems'

(ii) run system and operation jobs as required;

(iii) provide information to the Customer Support Team regarding the status of the systems; and

(iv) coordinatethe shutdown of the DR site operations and the transfer back to the Server room.

(5) Customer Support Team

(a) The Customer Support team provides assistance to the University community, customers and suppliers during the disaster from the time the disaster is declared until operations resume at the Server room.

(b) The pre-disaster responsibilities is to assist application customers during disaster recovery tests

(c) The disaster responsibilities and actions are:

(i) notifingparticipating application users that a disaster has been declared;

(ii) advisingusers of the disaster recovery system status, availability, and accessibility and

(iii) providingproblem diagnosis and resolution guidance/assistance to application owners and their users.

(6) Salvage/reclamation team

(a) The Salvage/Reclamation Team manages the restoration or rebuilding of the Server room. Itsmajor pre-disaster responsibility is to maintain current copies of equipment inventory lists, physical layout or diagrams (floor plans), and other pertinent documentation describing IT production hardware configuration in a suitable off-site location.

(b) The disaster responsibilities and actions are as follows:

(i) Oncethe restoration team has implemented recovery operations at the hot site, assess the damage to the Server room and report the damage, with recommendations, to the Executive Team.

(ii) Organize the recovery of salvageable equipment.

(iii) Initiate, coordinate, and expedite reconstruction to prepare the facility to receive equipment, supplies, tools, machinery, and utilities (electrical power, telephones, network connectivity, air conditioning, plumbing, water, gas).

(iv) Order and expedite replacements ofunusable IT equipment.

(v) Monitor the reconstruction of the new or repaired facility, and the installation of all utilities and other essentials.

(vi) Monitor the installation of computers, peripherals, and other IT equipment.

(vii) Advice the executive team regarding status, progress, and schedules, and any problems associated with the construction or reconstruction and installation.

(viii) Inform the executive team when the new or restored facility is ready for use.

(7) Disaster response

(a) In the event of a disaster, the Director, ICT,shall coordinate the following disaster recovery teams:

(i) Damage assessment team –to assess the damage of the ICT systems and determine if a disaster can be declared.

(ii) Executive team –to makes a decision to formally declare a disaster and establish a disaster command post with adequate communications and support equipment.

(iii)Restoration team –to restore the University's systems and applications at the DR site in preparation for continuationof normal operations for duration of the disaster.

(iv)Salvage/reclamation team –to reconstruct the servers at main server room.

(v) Operations team and restoration team –to conduct preparations to leave DR site and to resume operations at the main server room.

(vi)The Salvage/ reclamation team – to manage the restoration or rebuilding of the main systems and network infrastructure in the main server room.

(8) Testing disaster recovery site

(a) Regular testing ofthe disaster recovery plan shall be done to verify that the recovery procedures work as intended and that the supporting documentation is current and accurate, and determine whether personnel are adequately prepared to perform their assigned duties.

(b) The Director, ICT, shall schedule two DR site tests per year with sufficient time to test the operating system and application recovery procedures.

(c) The DR site tests shall be conducted and managed by members of the restoration, operations, and customer supportteams.

(9) **Disaster recovery teams**

(a) Damage assessment team

This team is composed of: Director ICT, Network Administrator, Systems Administrator, Database Administrator, Management Representative, and the Systems Engineer (consultants).

(b) Executive Team

This team is comprised of: Director ICT, Network Administrator, Systems Administrator, Database Administrator, and Management Representative.

(c) Restoration Team

This team is comprised of:Director ICT, Network Administrator, Systems Administrator, Database Administrator, Management Representative and Systems Engineer (consultants).

(d) Salvage/Reclamation team

This team is comprised of:Network Administrator, Systems Administrator I, Systems Administrator II and Computer Technologist.

(e) Operations and Restoration Team

This team is comprised of: Director ICT, Network Administrator, Systems Administrator and Database Administrator

PART XII. ICT IN THE LIBRARY

64. Guidelines for the use of ICT and electronic resourcesin the Library

(1) The following are recognisedas authorisedusers of library electronic resources:

(a) All members of SEKU staff.

(b) All SEKU students.

(2) **Online collections and services**

(a) The Library shall ensure SEKU is registered for the use of all subscribed databases.

(b) The Library shall market and promote all available e-resources to its users.

(c) The Library shall continually update the University community on new resources.

(d) Links to e-resources shall be made available on the Library website.

(e) The Library shall maintain a database of all electronic resources.

(f) The Library shall carry out training on e-resources from time to time.

(g) Users shall be sensitisedon implication of using scripts to down load articles from subscribed databases.

(3) **Management of database passwords**

(a) A database of passwords needed for the administration of ICT resources shall be maintained.

(b) Staff shall be assigned passwords and rights in line with their work requirements'.upon departure, passwords assigned to staff shall be disabled.

(c) Staff shall be responsible for passwords assigned to them.

(d) Users shall be sensitisedon the need to ensure passwords assigned for access to e-resources are not shared with unauthorized persons.

(4) **Communication**

The ICT related channels of communication shall be:

(a) Library website social media platform.

(b) SEKU corporate email.

(c) Any other approved university channels of communication.

(5) **ICT Human Resources Requirements**

(a) The ICT section shall consist of a System Administrator, a Systems Librarian, and anICT Technicians.

(b) The ICT Section shall be headed by a systems librarian who shall report to Deputy University Librarian in charge of Technical Services.

(6) **Maintenance and repair of Library ICT equipment**

(a) The maintenance of the library ICT equipment shall be carried out by the Directorate of ICT as stipulated by University regulations.

(b) The Library shall liaise with the Directorate ICT for the maintenance and repair of library equipment.

(c) All library staff shall be sensitized on the need for proper care and maintenance of the computers in their custody.

(7) **Purchase of Library ICT equipment**

(a) Purchase of ICT related equipment shall be guided by the regulations of the University's procurement procedures.

(8) **Data Security**

(a) The library shall work together with the Directorate of ICT to ensure security of all library electronic data.

(b) Back up of data shall be done on a daily basis in the server that is in the library.

(c) The systems librarian shall liaise with the Director ICT to ensure continuous and consistent back up of library data.

(d) Staff shall be sensitized to consistently back up important information in external disk

(e) Administrative passwords shall be changed from time to time.

(f) All computers shall be installed with anti-virus software to protect them against malicious software.

(9) **Online public access catalogue (OPAC)**

(a) The Library shallprovide terminals for access to the OPAC.

(10) **Management of digital laboratories**

(a) The digital library computer laboratories shall open for use as per the Library opening and closing hours.

(b) The digital library computers shallat all timesbe manned by ICT technician.

(c) All users shall be required to book for the use of computers in the laboratory.

(d) All students shall be allowed to occupy a terminal for a maximum of two hours

(e) The ICT technician assigned to work at the Library shall, in collaboration with the University Librarian, maintain an inventory of ICT equipment maintained by .

PART XIII. REVIEW OF POLICY

65. This Policy shall be reviewed from time to time to capture emerging issues of national, regional and global concern.

PART XIV. ANNEXTURES

APPENDIX I.
INTERNET USAGE ACKNOWLEDGMENT FORM

After reading this policy, please sign the Usage Acknowledgement form and submit it to the Director ICT.

By signing this form, you acknowledge that you shall comply with the Internet Usage Guidelines.

ACKNOWLEDGMENT

I have read the *Internet Usage Guidelines* and hereby attest that I understand the contentsand hence I agree to fully comply with the said *Policy*.

NAME: _____ Department: _____

Designation: _____ PFNo: _____

Signature: _____ Date: _____

Supervisor's Signature: _____ Date: _____

APPENDIX II

USER ACCESS MANAGEMENT FORM

Name: _____ Date: _____

Designation: _____ Type of Request:

Department: _____ New User □ Close Account □

Requested by: _____ Change Rights □

Email Account □

ERP Account □

Other □ _____

_____

_____

HEAD OF SECTION

Specify the rights to be assigned or withdrawn from the user.

	Administrative Rights
1.	
2.	
3.	
4.	

Period of access: _____

Reason for request: _____

_____

_____

_____

	USER	HEAD OF SECTION	DIRECTOR ICT	SYSTEMS ADMIN
Signature :	_____	_____	_____	_____
Date:	_____	_____	_____	_____

APPENDIX III

SOUTH EASTERN KENYA UNIVERSITY

DIRECTORATE OF INFORMATION COMMUNICATION AND TECHNOLOGY

Email: ict@seku.ac.ke **Tel:**+254-748-605-996/7 Ext: 256/7

ASSET MOVEMENT/ASSET TRANSFER FORM

RECEIVING DEPARTMENT: _____ FROM (DEPT. NAME):_____

DATE OF MOVEMENT: _____

#	ITEM DESCRIPTION	SERIAL NO.	SEKU-ASSET NO.	REASON FOR MOVEMENT	FILLED BY: NAME,SIGNATURE
1					
2					
3					

MOVEMENT AUTHOURISED BY:_____ _____ _____

NAME DESIGNATION SIGNATURE / DATE

ALL ASSETS RECEIVED AS INDICATED:_____ _____ _____

NAME PF/ID.NO SIGNATURE / DATE

NOTE: Attach: Delivery Note, LPO and/or Original Request which was approved

To be filled in Duplicate Original – ICT Copy