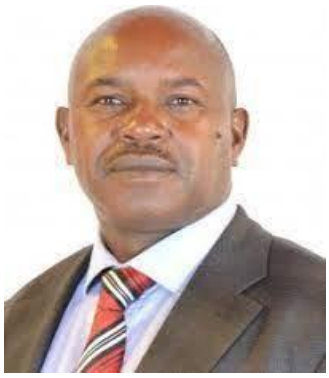
INFORMATION COMMUNICATIONS AND TELECOMMUNICATIONS POLICY

Wildlife Research and Training Institute
P.O. Box 842-20117, Naivasha, Kenya Telephone: (+254) 050 2020577
Mobile: (+254) 0700 000321 /0731 919 465
Website: www.wrti.go.ke
Email: director@wrti.go.ke, wrti@wrti.go.ke

FOREWORD



In line with its mandate in wildlife research and training, the Institute is embracing technology to enhance its operations. This requires robust ICT infrastructure to harness current and emerging technologies.

The Institute has adopted and continues to integrate ICT to fulfil its research and training goals. To guide this process, an ICT policy has been established to ensure optimal use of ICT resources, aligned with the Institute's strategic objectives and relevant national laws.

This policy outlines the objectives, principles, and strategies for integrating ICT into the Institute's operations. It also clarifies the purpose of ICT, while informing staff of associated risks, responsibilities, and benefits.

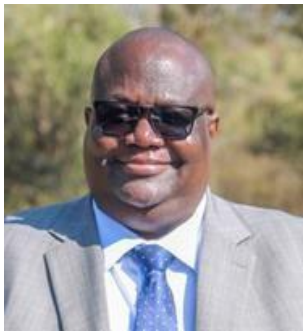
The ICT Policy is aligned with the Constitution of Kenya, the Kenya Information and Communications Act (Cap. 411A), the Data Protection Act (Cap. 411C), the Wildlife Conservation and Management Act (Cap. 376), the Institute's Strategic Plan (2024–2027), and the Bottom-up Economic Transformation Agenda (BETA).

Full implementation of this policy will foster innovation and position the Institute as a leading hub for wildlife research and development at national and international levels.

..... **DATE:** 16th May, 2025

DR DAVID NKEDIANYE
CHAIR, BOARD OF THE INSTITUTE

PREFACE



The objective of the ICT policy is to guide the integration of Information and Communications Technology at the Wildlife Research and Training Institute.

It recognizes the vital role of ICT in enhancing operational efficiency, service delivery, and the overall execution of the Institute's mandate.

The policy outlines guidelines for adopting and managing information systems, with a focus on the synergy between technology and human resource.

Staff play a key role in developing, operating, and maintaining these systems, making them central to successful ICT implementation.

By adopting this policy, the Institute aims to embrace modern technology and best practices, strengthen ICT governance, and empower staff to thrive in a dynamic, tech-driven environment.

We are confident that this policy will support the realization of the Institute's vision and mission by clearly defining responsibilities for its implementation and oversight.

..... **DATE:** 16th May, 2025

DR PATRICK OMONDI, OGW
DIRECTOR/CEO

TABLE OF CONTENTS

ACRONYMS

BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Assessment
BYOD	Bring Your Own Device
ERP	Enterprise Resource Planning System
HR	Human Resource
ICT	Information Communication & Technology
IoT	Internet of Things
ID	Identity
LAN	Local Area Network
MCA	Mission Critical Activities
PC	Personal Computer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCMD	Supply Chain Management Department
SIMS	Student Information Management System
WRTI	Wildlife Research and Training Institute
WAN	Wide Area Network

Definition of Terms

ICT (Information and Communication Technologies): ICT means technology, including computers, telecommunication and audio-visual systems, that enable the collection, processing, transportation and delivery of information and communications services to users.

A Vision Statement: A ***Vision statement*** outlines what an organisation aims to be. It concentrates on future; it is a source of inspiration. An ICT Vision statement defines where the department wishes to be in relation to deployment of ICT in support of teaching and learning.

ICT Mission: A ***Mission statement*** is a general statement of the overall purpose and aims of the ICT policy and strategies. It concentrates on present; it defines the customer(s), critical processes and the desired level of performance. It is a progressive roadmap towards the attainment of a vision.

ICT Policy: a deliberate plan of action to guide decisions and achieve rational outcome(s). Policy differs from rules or law. While law can compel or prohibit behaviours policy merely guides actions toward those that are most likely to achieve a desired outcome.

ICT System: An ICT system includes, but is not limited to, hardware, software and communications equipment that the Institute uses to communicate, process and store information. The organization and structures involved in relating all these systems, the information they store and the people involved in the administration and maintenance.

User: any person who is recognized by the Institute as having a valid reason to access the Institute ICT systems whether that access is from within the Institute or outside the Institute

Alternate Site: means a site held in readiness for use in the event of a major disruption that maintains an organisations' business continuity.

Business Continuity: means a state of continued, uninterrupted operation of a business.

Business Continuity Management: means a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can

be maintained or recovered in a timely fashion in the event of disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.

Business Continuity Plan: means a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organisation in the event of a disruption.

Business Impact Analysis: means the process of identifying, and measuring (quantitatively and qualitatively) the business impact loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements and essential staff and to help shape the business continuity plan. All impacts should be measured on financial, regulatory, legal and reputational damage basis.

Call Tree: means a system that enables a list of persons/roles/organizations to be contracted as part of an information/communication plan.

Communication Protocols: means an established procedure for communication that is agreed in advance between two or more parties internal or external to an institution. Such procedure also includes the nature of the information that should be shared with internal and external parties and how certain types of information should be shared with internal and external parties.

Critical Services: means any activity, function, process or service, the loss of which would be material to the continued operation of a financial institution.

Crisis: means an event, occurrence and/or perception that threaten the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an institution.

Crisis Management Team: means a team consisting of key executives, key role players (i.e. legal counsel, facilities manager, disaster recovery coordinator), and the appropriate business owners of critical functions who are responsible for recovery operations during a crisis. Evaluation of capability, training, testing of Crisis Management teams maturity level shall be documented.

Disaster: means a sudden, unplanned catastrophic event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time, causing unacceptable damage or loss.

Emergency Response Team: means any organization that is responsible for responding to hazards to the general population (e.g. fire brigades, police services, hospitals)

Exercising: means the process through which business continuity plans are tested and rehearsed in a controlled environment using team members and staff.

Major Operational Disruption: means a high impact disruption of normal business operations, affecting a large geographic area and adjacent communities that are economically integrated to it.

Operational Risk: means the risk of loss from inadequate or failed internal processes, people and systems or from external events.

Recovery: means the rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.

Recovery Objective: means a predefined goal for recovering specific business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption (recovery time).

Recovery Time Objective (RTO): means the duration of time required to resume a specified business operation. It has two components, the duration of time from activation of the business continuity plan and the recovery of business operations.

Recovery Point Objective (RPO): means a point in time to which data, shall be restored from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a disruption.

Resilience: means the ability of an organisation, network, activity, process or financial system to absorb the impact of a major operational disruption and continues to maintain critical operations or services.

Risk Assessment: means the probability and impact of specific threats being realised.

Single Point of Failure: means a unique source of a service, activity, and/or process where, there is no alternative and whose loss could lead to the failure of a critical function.

Administrators –means a person responsible for management of a particular aspect of ICT resources

Manager/ Supervisor: means a person overseeing overall ICT resources in managing access rights and work allocation.

User: means any person authorised by way of access rights to use an ICT resource.

Portal: means an organisation's data/information resource accessed via internet for public usage.

1.0: INTRODUCTION

1.1 The Institute is a Government Research and training Corporation mandated to coordinate and undertake wildlife research and training in the country in accordance with section 51 of the Wildlife Conservation and Management Act.

1.2 The Institute was established with the mandate to provide reliable scientific information on emerging wildlife conservation and management challenges and enhance capacity in the wildlife sector through training.

1.3 This ICT policy shall guide the Institute in managing Information Technology, which is a very dynamic sector, and with technology continuously developing and advancing, it is imperative that the Institute develops an ICT policy to help manage Information Technology trends.

1.4 This ICT policy is set out to provide guidelines and procedures to WRTI members of staff and third parties on matters related to ICT use, and also to ensure compliance to the same.

1.5 The ICT policy will facilitate efficient and effective service delivery through timely provision of a robust ICT infrastructure, application software, support services and operational capacity.

2.0 Strategic Intent and Purpose

2.1 The intent and purpose of this policy is to;

(a) mainstream ICT in the Institute;

(b) guide the seamless integration of ICT infrastructure in the Institute's Mandate;

(c) facilitate acquisition and management of ICT Infrastructures;

(d) guide on the adherence to best ICT practices & policies; and

(e) promote the digital transformation.

3.0 Scope of ICT Policy

3.1 This policy shall apply to the Institute's employees, trainees and stakeholders, suppliers, contractors and service providers.

4.0 Governance Framework

(a) Board of the Institute
(b) Director/CEO
(c) Digitilization Committee
(d) Head of ICT
(e) Staff

5.0 Legal Framework

I. Constitution of Kenya.
II. The Computer Misuse and Cybercrimes Act (Cap. 79C).
III. Kenya Information and Communications Act (Cap.411A).
IV. The National ICT Policy.
V. Data Protection Act (Cap.411C).
VI. Access to Information Act (Cap.7M).
VII. Environmental Management and Co-ordination (e-waste management)Regulations,
VIII. The Copyright Act(Cap.130).
IX. Other relevant legal provisions and Government policies that may come into force after initial implementation of this ICT Policy.

6.0 Roles and Responsibilities

6.1 Board of the Institute

The board shall—

(a) give policy direction on data management and data protection in the Institute;
(b) give guidance on the policy direction, provide budgetary allocation for its implementation and conduct implementation oversight;
(c) ensure the ICT policy is aligned to the objectives of the Organization;
(d) establish an ICT function in the organization;
(e) integrate ICT in the operations of the organization;
(f) put in place a Business Continuity Plan;
(g) ensure ICT related risks are identified and managed; and
(h) utilize ICT in monitoring the performance of the organization.

6.2 The Director/Chief Executive Officer

The Director/Chief Executive Officer shall—

(a) provide the overall leadership in the adoption and implementation of the policy;

(b) appoint a Digitalization Committee to guide on the implementation of this policy; and

(c) provide resources for the implementation of this policy.

6.3 Digitalization Committee

The Digitalization Committee shall be responsible for overall strategic management and monitoring of ICT resource allocation, utilization and overseeing the implementation of ICT projects.

6.4 Head of ICT

The Head of ICT shall—

(a) in liaison with Heads of Directorates and Departments, ensure that all users are sensitized and comply with the policy;

(b) undertake monitoring and evaluation of this policy; and

(c) ensure that ICT resources supplied meet or exceed the minimum requirements.

6.5 The Staff

The Staff shall—

(a) adhere to the ICT policy; and

(b) report any attempted security breaches.

7.0 Objective of ICT Policy

The objective of the ICT Policy is to—

(a) facilitate the development of ICT skills to support ICT systems in the Institute;

(b) support and encourage innovations in technology development;

(c) support the use of technology and general work flows within the Institute;

(d) promote information sharing within the Institute and towards the general public;

(e) promote efficient communication among the Institute's staff, students and stakeholders; and

(f) ensure that ICT facilities are fully accessible to users with special needs.

8.0 Policy Statement

8.1 The Institute is committed to creating an environment for the digital transformation by leveraging ICT in compliance to the relevant Kenyan laws.

8.2 The Institute shall continuously support the Digital transformation by adopting modern technologies and skills development

9.0 Rationale

9.1 This policy provides guidelines to the Institute in ensuring that ICT is integrated in its operations.

9.2 The policy will also ensure that ICT technology is put in place in compliance with the relevant ICT standards, laws and regulations.

10.0 Policy Guidelines

This policy shall be implemented through the policy guidelines as outlined in the Annexures.

i. ICT Governance.
ii. ICT Infrastructure.
iii. ICT Software's.
iv. ICT Security.
v. Network Management.
vi. ICT Services Management.
vii. ICT Business Continuity.
viii. ICT Health and Safety.
ix. Prohibitions, Restrictions and Penalties.

11.0 Policy Implementation

The Institute shall use the existing administrative structures to implement this policy.

12.0 Policy Review

This policy shall be reviewed every three years or as need arise.

ANNEXURES

ANNEX 1: ICT GOVERNANCE

For effective governance, the Institute management shall establish a Digitalization Committee (DC) with clear terms of reference.

1.1 Establishment of the Digitilization Committee

The Director/CEO in consultation with management shall establish and appoint members of the Digitalization Committee.

1.2 Role of the Digitalization Committee

The Digitalization Committee shall—

(a) ensure that the Institute plans for ICT support in line with the WRTI strategic goals.

(b) advise Management on ICT matters and support the Head of ICT in growing ICT as a tool to enable 21st Century Research and Training practices, support management and strategic direction of the Institute.

(c) help provide an enabling environment for effectiveness by teaching staff, management and leadership at WRTI as an integral part of all operational activities.

(d) foster integration of ICT into broad Institute.

The Digitalization Committee will provide oversight support to the head of ICT by:

(a) Establishing a shared vision on ICT that add value to the Institute.

(b) Establishing the Institute's ICT goals and strategies for achieving the vision and goals.

(c) Establishing principles and guidelines for ICT decision making and managing ICT initiatives.

(d) Guiding the principles and processes by which ICT projects will be executed

(e) Enhancing support for ICT policy, programs, contracts and projects through active participation

(f) Providing input to the formation of new policies, contracts and systemic projects.

(g) Identifying and setting project priorities

(h) Providing input for increasing efficiency and effectiveness of professional ICT related activities at WRTI.

(i) Collaborating with the head of ICT to provide general feedback when necessary.

(j) Engaging the CEO/DDs/Head-ICT requests for information about or investigation of specific ICT issues;

(k) Supporting the head of ICT in the conduct of specific research and project tasks as required.

1.3 TASKS AND RESPONSIBILITIES

1.3.1 Consideration of Proposed Projects

The Digitalization Committee will consider all ICT projects proposed for the Institute, and shall maintain a register of these projects. The committee will ensure that the criteria is met, including by ensuring proposals have been prepared, the costs and return on in investment to WRTI are clearly documented, and that start up and ongoing operational costs, including staffing are covered.

In considering all projects, consideration shall be given to WRTI strategic plan, Knowledge Management & Information Management strategies and information and technical architectures, to ensure that projects are consistent with these broader frameworks and advance the goals articulated in them.

1.3.2 Identify and Set Priorities

The committee will consider all the proposals put to it and make a recommended prioritized list, based on the merits of the individual project cases and wider institutional context. The Chief Executive Officer shall assess and determine funding priorities within the context of a wider Institution strategic view of priorities for all capital spending.

1.3.3 Review Projects in Progress

The Digitalization Committee will oversee projects and prepare reports, which shall be submitted, to the Chief Executive Officer. Oversight shall include risk review, financial review, and achievements against the plan.

1.3.4 Guidelines

The responsibility for ICT service delivery, projects management, financial planning and operational management remains with the head of ICT.

1.4 MEMBERSHIP CRITERIA

The members of the Digitalization Committee shall be appointed by the Director/CEO.

1.5 . REVIEW OF TERMS OF REFERENCE

The Institute Management shall review the Digitalization Committee's Terms of Reference every two years.

ANNEX 2: ICT INFRASTRUCTURE

2.1 ACQUISITION OF ICT ASSETS

2.1.1 Purpose
This policy shall guide the Institute on acquisition and ownership of ICT resources.

2.1.2 Scope
This policy provision applies to all ICT resources acquired through procurement or under MOUs/grants/donations/agreements/gifts and the ownership transferred to the Institute.

2.1.3 Provision
(i) All ICT resources acquired by the Institute shall belong to and remain as property of the Institute.

(ii) All ICT resources acquired by the Institute under Grants/MOU/Agreements /Donation shall have elaborate terms and conditions which include and specify ownership.

(iii) The Institute will be responsible for purchasing the ICT resources for projects and where the Institute receives ICT equipment as a donation, they shall undergo full scanning and re-configurations as per the Government's directive.

(iv) The ICT Department shall provide technical specifications for the acquisition of ICT resources.

(v) All ICT resources acquired shall be coordinated with the ICT Department to ensure that it conforms to corporate standards.

2.1.4 Guidelines
(i) All requisitions for procurement of hardware, software and specialized equipment shall be channeled through the ICT Head.

(ii) Technical specifications will be provided by the ICT Department according to the user needs.

(iii) In acquisition of ICT resources, the ICT Department shall be involved in the procurement process that includes evaluation, inspection and acceptance/rejection.

(iv) The ICT Department shall ensure all ICT resources are installed, configured, tested and commissioned as per the requirements.

(v) ICT, Assets Office and SCMD shall ensure that all ICT equipment procured by or granted to the Institute shall be identified as belonging to the Institute, tagged or engraved for identification purposes before distribution.

(vi) At distribution, all details shall be captured by Assets Officer into a digital asset inventory and copy maintained by ICT Department, assets officer and Administration office.

(vii) The ICT Department shall use best practice and global standards and guidelines to develop technical specifications.

(viii) All software acquired shall have accompanying licenses and user manuals.

(ix) There shall be an ICT Equipment register to log the movement of equipment to and from the Department.

(x) Inventory of the machines which are out of warranty shall be maintained.

2.2 ICT HARDWARE UTILIZATION

2.2.1 Purpose

The purpose of this provision is to protect and maintain ICT hardware in the Institute so as to derive maximum value for the intended use and enhance efficiency and effectiveness in employees' job performance.

2.2.2 Scope

The policy provision shall apply to all hardware in the Institute. The hardware includes: Personal Computers, Tablets, iPads, Mobile Phones, Printers, Servers, Scanners, Projectors, photocopiers, UPS, network switches, access control, CCTV, Digital Cameras among others.

2.2.3 Role of Department

a) The ICT Department shall facilitate the acquisition, installation, configuration, testing, training and maintenance of ICT equipment in the Institute as follows:

3.2.3.1 New ICT Hardware

(i) All ICT assets shall be recorded in an electronic inventory register and identified individually.
(ii) Users shall be required to sign for the ICT items as they are being issued to them.
(iii) Users should be allocated new hardware in accordance with the following eligibility levels.
(iv) Laptops, personal computers, printers and scanners will be issued to all levels of employees based on the following yearly user requirements.
(v) Departmental/Directorate heads should forward their staff requirements to H/ICT for consideration and planning.
(vi) IT support staff shall verify the need for user hardware replacement or disposal.
(vii) All the recommendations for user hardware replacement or disposal shall be forwarded to H/ICT.

2.2.3.2 Returning ICT Hardware

(i) Users shall be issued with a clearance form which shall be signed upon returning any issued ICT Hardware.

2.2.3.3 ICT Hardware Movement

(ii) Any ICT equipment leaving any WRTI facility either for repair or being carried away by a third party or contractor shall be issued with a gate-pass.

(iii) Returned hardware shall be verified to ascertain that it is in its intended condition before being accepted.

2.2.3.4 Retirement of Obsolete ICT Hardware

(i) The process of technical evaluation of ICT hardware to determine whether it is more economical to repair, upgrade, replace or decommission shall be done annually or upon approval by H/ICT for the purposes of disposing obsolete equipment.

(ii) ICT hardware shall be considered obsolete if the estimated cost of repair, maintenance or upgrade exceeds one–half of the current replacement value or they are damaged beyond repair.

(iii) ICT hardware such as Mobile phones and tablets, laptops that have surpassed their three (3) years will be accessed by the ICT department for recommendation for upgrade, re-allocation or disposal as per the Assets policy.

(iv) ICT hardware and their accessories are considered uneconomical to maintain if the total cost of running them exceeds 60% of the cost of replacement and compatible replacements are not readily available.

(v) Obsolete ICT hardware shall be disposed of as stipulated by the Public Procurement and Assets Disposal Act.

2.3 ICT ASSETS REPAIR AND MAINTENANCE

2.3.1 Purpose

The purpose of this provision is to provide for systematic inspection, upgrade, downgrade, detection, reconfiguring, modifying, replacing or changing and servicing. Maintenance includes but not limited to software changes, hardware changes, network changes, patches or cabling.

2.3.2 Scope

The policy provision shall cover all ICT computing infrastructure and accessories.

2.3.3 Provision

(i) The Institute shall ensure that preventive, corrective and adaptive maintenance plan is undertaken.

(ii) The Institute shall ensure that the maintenance contracts and preventive plans are reviewed periodically to ensure that they meet the required standards.

(iii) The Institute shall plan and have quarterly maintenance of ICT equipment and systems.

2.3.4 Guidelines

(i) Any break down and/or malfunction of the ICT computing infrastructure shall be reported to the ICT Department through Directorates and departmental heads.

(ii) Repair and maintenance of ICT computing infrastructure shall be coordinated by Head ICT Department. Where repair and maintenance is to be performed by an external entity, the Head ICT Department shall advice accordingly.

(iii) The ICT Department shall maintain documentation and inventory of repairs and maintenance for the Institute.

(iv) ICT, SCMD and legal directorates shall prepare and maintain documentation and contracts on all ICT computing infrastructure undertaken by the Institute.

(v) ICT Department shall test and accept ICT computing infrastructure repaired and maintained by preparing an acceptance report.

(vi) Written notice of all scheduled maintenance of a significant nature shall be provided to all Institute's staff /Public stating the nature of changes, system impact as well as documenting the static time and duration of the maintenance.

(vii) The ICT department shall develop guidelines on the ICT resources usage by the trainees.

2.4 ICT ASSETS AND SERVICE WARRANTY

2.4.1 Purpose

The purpose of this provision is to ensure that the warranty given to the Institute by contractors and suppliers confirms that an ICT product or service is reliable and free from defects is kept, and that the contractor/supplier will, without charge, repair or replace defective parts within a given time limit and under conditions agreed upon.

2.4.2 Scope

This policy provision shall cover all ICT resources acquired by the Institute.

2.4.3 Provision

(i) All ICT resources acquired by the Institute shall come with a written warranty.

(ii) The Institute shall undertake to ensure warranties are honoured.

2.4.4 Guideline

(i) During preparation of ICT equipment specifications, warranty requirement and period shall be clearly defined.

(ii) During delivery and inspection of ICT equipment, the Head of the ICT Department shall ensure that the warranty is provided for as per the specifications.

(iii) All ICT equipment shall come with a warranty from the manufacturer or supplier.

(iv) Contractors for ICT equipment/services shall be authorised dealers and have manufacturer's authorisation.

(v) The ICT Department shall verify the part numbers of all ICT equipment with the manufacturer where applicable.

2.5 E Waste Disposal

2.5.1 Purpose

The purpose of this provision is to provide guidelines for the disposal of ICT equipment.

2.5.2 Scope

This policy provision covers ICT equipment owned or operated by the Institute.

2.5.3 Provision

(i) All ICT computing infrastructure that cannot be reused or serviced shall be forwarded to the ICT Department for assessment before forwarding for disposal by SCMD.

(ii) All disposed ICT computing infrastructure shall be recorded and the asset inventory updated accordingly.

2.5.4 Guidelines

(i) All ICT equipment shall only be disposed of after making sure that all the data or information is backed up and permanently erased where applicable.

(ii) All ICT storage media shall be disposed of by demagnetizing and or physically destroying them.

(iii) All ICT equipment to be disposed of shall be certified by Head ICT as obsolete.

(iv) Disposal of ICT equipment shall be undertaken by the Supplies Chain Management department according to the Public Procurement and Assets Disposal Act (Cap. 412 C).

(v) ICT equipment have a lifespan after which a process for its disposal shall be put in place by ICT and SCMD.

(vi) ICT equipment assigned to individual staff members shall be disposed after being deemed unusable by the ICT department.

(vii) ICT equipment that are considered personal i.e., Mobile phones and tablets shall be decommissioned as per the Public Procurement and Assets Disposal Act.

ANNEX 3: ICT SOFTWARE

3.2.2 Purpose

To ensure that software used in the Institute is in compliance with applicable licenses laws, notices, contracts and agreements to safe-guard the Institute against any legal implications, benefit from support provided by the licenses.

3.2.3 Scope

This policy provision applies to all software's developed or acquired for the purposes of the Institutes' business functions. These include: operating systems, application software, database software, customized /off the Shelf software, computer drivers, Antivirus and source code.

3.2.4 Role of Department

(i) All ICT equipment acquired and used in the Institute shall run on genuine and licensed software.

(ii) All software acquired for or developed on behalf of the Institute shall be the property of the Institute.

(iii) All software licenses shall be installed and managed centrally by the ICT Department through Active Directory Environment or Central Console.

iv) Source code for all application software developed for the Institute shall be the property of the Institute.

3.2.5 Guidelines

(i) Users shall request for software through the ICT head.

(ii) ICT head shall maintain records of software licenses owned by the Institute.

(iii) ICT Department shall periodically scan computers to verify that only authorised software is installed.

(iv) All software is managed by the ICT Department in accordance with the provisions of the software licenses.

(v) Institute's staff shall be individually responsible for reading, understanding and following applicable licenses, notices, contracts and agreements for software usage on Institute computers. The staff shall not:

(a) Install software without authority by the ICT Department.

(b) Duplicate software.

(c) Download software unless authorised by the ICT department.

3.2.6 Release of Software

i) Institute's Software shall not be loaned, traded, sold, given away, or otherwise divulged.

ii) Any upgrading, downgrading and updating of software will be done by the ICT Department.

3.2.7 Custody of the software

(i) ICT Department shall have custody of all software in the Institute.

(ii) ICT Department shall facilitate training on the acquired software where necessary.

(iii) The Institute staff shall not borrow or lend any software without the consent of Head ICT.

(iv) All software developed in house by the WRTI staff/on-job trainees shall become the property of the Institute. There shall be due recognition of innovativeness by the issuance of an Innovation Certificate.

3.2.8 Licenses

(i) The Institute shall comply with all laws regarding intellectual property. This applies to all Software licensed or developed in the Institute.

(ii) The Institute may negotiate for corporate licenses where necessary.

(iii) All purchased/customized software shall be accompanied by the required licenses as per specifications.

(iv) All acquired/customized/revision software shall be delivered with documentation.

3.2.9 Source Code

It shall be the obligation of the contractor to provide the source code to the Institute and ensure that updates are provided when changes are made on the systems.

3.2.10 Renewal of support licenses

The ICT Department shall negotiate for the renewals of licenses on behalf of the Institute in liaison with the user Department and SCMD.

3.3 ICT Intellectual Property Rights

3.3.1 Purpose

To protect the possibility of inadvertent infringement of the Intellectual Property Rights of software developed in-house or by third parties using or implementing the Institute customized specifications.

3.3.2 Scope

All system developers, employees of the Institute and all third parties contracted to develop software and systems for the Institute.

3.3.3 Provision
All systems and software developed for the Institutes' use shall be a copyright of the Institute as well as per the guidelines on the Intellectual Property Policy.

3.3.4 Guidelines
(i) Third party copyrighted software used by contractors engaged by the Institute as third party software shall retain copyright ownership of its original work, while at the same time granting the Institute a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Contractor's copyrights in its project delivery to reproduce, distribute, publish, display, perform, and create derivative works of the project based on that original work for the purpose of developing software or systems under the Institute 's copyright.

(ii) Users accessing web-based applications using the internet are not permitted to use false information or copy, transfer, rename, add or delete programmes belonging to others unless given express permission to do so by the owner.

(iii) Users shall observe copyright or license agreements.

3.5 Service Level Agreement (SLA)

3.5.1 Purpose
To ensure provision, performance and availability of ICT services and systems at all times. The Service Level Agreement (SLA) will be contracts between service provider(s) and the Institute. The SLAs shall specify in measurable terms, the availability, timeliness and performance criteria that the contractor is intended to meet while delivering service and sets out the remedial action and penalties in case of violation.

3.5.2 Scope
The SLAs shall cover ICT computing infrastructure.

3.5.3 Policy
SLAs shall be prepared, discussed and negotiated by ICT department in conjunction with the relevant actors.

3.5.4 Guidelines
(i) The SCMD in collaboration with legal office from the Institute shall ensure that SLA contract documents meet the required contractual standards before signing.

(ii) SLAs shall be reviewed on need basis.

(iii) External service providers shall sign a non-disclosure agreement with the Institute when carrying out maintenance and repair services.

(iv) Developed/acquired system contracts shall be maintained by the contractor/vendor/supplier for a specified period of time.

ANNEX 4: ICT Security

ICT security is divided into two main categories, that is; physical security and logical security.

4.1 Physical Security

4.1.0 Purpose

To prevent unauthorised access or damage to hardware, software and information. This encompasses misuse, malicious or accidental damage, vandalism, intrusion, theft, undesired access and sabotage as well as natural disasters such as fire, water or earthquakes. This policy shall ensure confidentiality, integrity and availability of data in case of unforeseen harmful events.

4.1.1Scope

The ICT security policy shall address security with regard to physical and environmental facilities, ICT equipment, network infrastructure, staff and third parties.

4.1.2 Policy

(i) The Institute shall provide access control and surveillance for the ICT key installations such as Data Centre, active devices, cabinets and fibre channels.

(ii) Data Centres shall be restricted areas, away from normal operations and only accessible to authorised personnel.

(iii) Access control systems shall incorporate the use of biometrics and access cards for authentication.

4.2 CCTV

4.2.1 Purpose

The specific purpose of enhancing the safety and well-being of staff, WRTI assets and visitors. The planning and design of CCTV systems will endeavour to ensure maximum effectiveness and efficiency.

4.2.2 Scope

This policy applies to all WRTI premises where the installation has been implemented by the Institute.

4.2.3 Policy

(i) Security and ICT Department shall ensure footage can be given out to management on request basis through writing to ICT Head. This can be done through authorisation from Human Resource and administration directorate.

(ii) Security and ICT Department shall ensure CCTV footage is accessible as and when required.

(iii) Security and ICT Department shall ensure Back-up of CCTV footage is maintained as per Institute's back-up processes and procedures manual.

(iv) Security and ICT Department shall ensure that the CCTV footage is retained/archived for a period of 90 days in accordance with the Public Records and Documentation Act.

4.2.4 Guidelines

The following guidelines are to help in monitoring of the CCTV systems;

(i) The CCTV cameras shall be used to capture footage/ images of events/ occurrence within the Institute.

(ii) The recorded events/ occurrences shall not be used for any commercial purposes.

(iii) The recorded images shall only be released to a third parties upon receiving written approval by the Institute.

(iv) The day-to-day monitoring of the CCTV shall be the responsibility of the security officers of the Institute.

(v) Assigned ICT officers shall be responsible in the management of technical aspect of the CCTV system by ensuring uptime of the system.

(vi) The footage shall be retained for a maximum period of 30 days.

(vii) Incidents that require retrieval of the footage shall be reported within 7 days.

4.3 Access Control

4.3.1 Purpose

Secure access for the purpose of identifying employees and giving access entries to the WRTI premises.

4.3.2 Scope

This policy applies to all Institute's premises, staff and other stakeholders.

4.3.3 Policy

(i) All WRTI applications and systems shall be defined to operate with an appropriate access control mechanism to ensure that only authorized users can use them for permitted purposes.

(ii) Users shall only be allowed to access critical business information assets and processes required to perform their job responsibilities.

(iii) Any system that handles confidential information shall be protected with a password-based access control system.

(iv) Any system that handles highly confidential information shall be protected by a multi-factor-based access control system for enhanced security.

(v) A discretionary access control list shall be in place to control access to resources for different groups of users.

(vi) ICT Department shall ensure biometric data/information can be given out to management or any other party/parties on request basis through writing to ICT Head. This can be done through authorisation from Human Resource and administration directorate.

(vii) All staff/interns/attachees/temporary staff shall be required to be enrolled in the Biometric/access card for purpose of gaining access to the Institute's premises.

(viii) Biometric data/information reports on users gaining access to the Institute's premises can be given out to management upon request basis through writing to ICT Department.

(ix) ICT Department shall ensure that the Access control logs is retained/archived for a period of 90 days in accordance with the Public Records Act.

4.4.4 Guidelines

(i) All staff/interns/attachees/temporary staff shall be required to produce employment/transfer/deployment/secondment letter or staff ID card to ICT Department for enrolment into the Biometric system.

(ii) Human Resource and Administration Directorate shall communicate through writing to ICT Department staff who have resigned, suspended, expelled, retired and interdicted to be disabled/deactivated from the biometric system.

(iii) Assigned ICT officers shall be responsible in the management of technical aspect of the Biometric system by ensuring uptime of the system.

(iv) The Access control logs shall be retained for a maximum period of 90 days.

Access to Data Centre

(i) Physical access to the Data Centre area shall be controlled. Unauthorised persons shall not access the Data Centres

(ii) Doors to Data Centres shall be kept locked at all times and posted with "Restricted Area-Authorised Staff Only" signs. Only authorised staff shall be assigned biometric access to these areas. Other staff shall be provided limited access on a need-to-enter basis.

(iii) All visiting delegations shall have prior appointments and shall be accompanied by an authorised officer within these restricted areas.

(iv) All entries and exits of every visitor and third parties shall be logged in a register which is always maintained at the entry of the Data Centre.

(v) Contractors/suppliers shall be accompanied by authorised officers and shall enter their details in the entry/exit register.

(vi) Visitors are prohibited from taking photographs and videos within the data centre.

(vii) Eating and drinking in the server room is prohibited.

(viii) The data centre shall be equipped with fire suppression and detection systems, fire extinguishers, air conditioning, backup power as per international best practices.

(ix) Proper dressing shall be observed in the server room in order to comply with the SHE requirements.

Data Centre Environment

(a) **Hand-held** fire extinguishers shall be placed in strategic positions in the Data Centres. They shall be tagged for inspection and inspected annually.

(b) **Smoke Detectors** shall be placed above and below the ceiling tiles throughout the facility and below the raised Data Centres. They shall produce an audible alarm when activated.

(c) **Fire suppressors** shall be installed that removes oxygen from the air, thus starving the fire. The system should not damage the equipment.

(d) **Regular inspection by the contractors or suppliers** shall ensure that all fire detection systems comply with building codes. The relevant department shall inspect the system and facilities annually.

(e) **Fireproof walls, floors and ceiling** surrounding the Data Centres shall contain or block fire from spreading. The surrounding walls shall have at least a two-hour fire resistance rating.

(f) **Emergency power – off switch** to computers and peripherals shall be shut off in case of an emergency evacuation.

(g) **Data Centres** should have raised floor, floor tiles and not carpeted to minimize dust.

Access to GIS /Computer Lab / Innovation Hub

(i) Only authorised staff shall work full time in computer lab.
(ii) Other staff, vendors and maintenance personnel shall be provided with limited access on a need-to-enter basis.
(iii) All visitors to the GIS/computer lab shall be escorted by an authorised staff and shall accompany the visitor until they depart.
(iv) GIS/Computer lab shall be locked when staff are not present, and the equipment shall be switched off at end-of-day or when not in use for extended periods.

Theft Prevention of ICT equipment

All theft or attempted vandalism shall be reported to the forensic and investigation unit by the affected party for investigation and further necessary action.

ICT equipment shall not be removed from Institute's premises without authorisation by the respective Heads of Directorates/Departments.

Remote data access

(a) The Institute shall have procedures for remote data access.

(b) Remote data shall only be accessible through the Institute VPN managed by the ICT department

(c) ICT personnel will connect the users to the VPN based on rights and procedures defined and approved by head of ICT.

(d) ICT Personnel shall take reasonable precautions to ensure remote access connections are secured from interceptions and eaves dropping or misuse.

(e) The Institute data handling procedures including access rights shall be applied while accessing remote data.

Classifying the Institute data

Institute data shall be classified based on its sensitivity, availability, confidentiality and integrity levels. The Institute data shall be classified in several levels which include: Critical data, restricted data, and Institute internal and public data.

(a) Critical data

(i) This shall be classified as data which if handled inappropriately or disclosed it could cause severe harm to individuals and the Institute.

(ii) The harm to the Institute will range from exposure to criminals, identity theft, financial loss and invasion of privacy. Such information shall include, Institute bank statements, credit cards.

(b) Restricted data

(i) This shall be classified as data whose disclosure could cause significant harm to individuals of the Institute and the Institute.

(ii) The harm can be exposure to civil liability due to the legal and ethical issues

(iii) This data shall be accessed with authorization.

(iv) Only selective access may be granted. This data shall include financial aid data, Students transcripts.

(c) Institute Internal Data

(i) This shall be classified as data whose disclosure causes limited harm to the Institute and individuals.

(ii) The data may be accessed by employees and other designated eligible employees of the Institute for the purposes of the Institute.

(iii) Access restriction should be applied for this data. Such data shall include financial reports, departmental memos and committee meetings.

(d) Public Data

(i) This shall be classified as Institute information whose disclosure possess little to no risk to individuals of the Institute.

(ii) There are very few restrictions placed to this data and are available to members of the public upon request.

(iii) It is also published to the public. This data shall include Institute websites, news releases information subject to open records requests like emails, financials etc.

4.4 Cyber Security

4.4.1 Purpose

Defending users, computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

4.4.2 Scope

This policy provision applies to all Institute ICT assets, staff and other stakeholders using Institute's ICT resources

4.4.3 Policy

(i) The ICT Department shall develop and ensure that a detailed information security strategy document is developed to guide on best practices on prevention of cybercrime in the Institute.

(ii) The ICT Department shall ensure that staff in the Institute are protected by implementing mechanism to prevent fraud, scam, phishing and other forms of infiltration.

(iii) Only authorised users shall be allowed to access information on the Institute's network. All service providers shall meet the security requirement as prescribed in this policy.

(iv) The ICT Department shall ensure that the Internal ICT systems are not a source of cyber risk by ensuring the data exchange procedures between systems comply with all security requirements and best practices.

4.4.4 Guidelines

Auditors shall be granted access to ICT resources for the purpose of performing systems audit when needed.

4.4.5 Remote Access

(i) WRTI Staff, contractors, vendors, and agents with remote access privileges to WRTI's corporate network are responsible for ensuring that their remote access connection is treated with the same consideration as the user's on-site connection to WRTI.

(ii) General access to the Internet through the WRTI network is strictly limited to WRTI Staff, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the WRTI network from a personal computer, Performance of illegal activities through the WRTI network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for the consequences of misuse of the Authorized User's access.

(iii) All offsite WRTI users wishing to connect to the WRTI network shall do so through the VPN connection provided by the ICT Department.

(iv) Authorised Users shall protect their login and password, even from family members.

(v) While using a WRTI-owned computer to connect to WRTI's corporate network remotely, authorised users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or the complete control of an authorised user or third party.

(vi) Users shall have the required authorisation to access internal resources from remote locations. Remote access for an employee, external user, or partner can be requested only by the manager responsible for the information and granted by the ICT Department.

(vii) All hosts connected to the WRTI internal networks via remote access technologies, including personal computers, shall use the most up-to-date anti-virus software.

(viii) Personal equipment used to connect to WRTI's networks shall meet the requirements of WRTIowned equipment for remote access.

(ix) Remote access tools shall support robust and end-to-end encryption of the remote access communication channels.

(x) Non-staff requests for remote access should be authorised only in cases where there is a justifiable business need. Such Access will only be granted upon the joint approval of the Head of the Department and HOD of ICT.

(xi) Access for non-staff, contractors, consultants, or vendor personnel should include a signed Non-Disclosure Agreement (NDA) as an integral part of the principal approval.

(xii) Vendors and other third parties requiring remote access to WRTI information systems shall have remote access provided for a defined and specified period, after which access shall be revoked.

4.5 Password

4.5.1 Purpose

To protect and control access by users to ICT resources, systems and to establish a standard for creation and management of passwords and user accounts.

4.5.2 Scope
This policy applies to all users, networks and systems at the Institute.

4.5.3 Policy
(i) All ICT resources shall be protected by use of passwords, access levels and segregation of duties'.

(ii) There shall be defined access levels, responsibilities, user rights, roles and privileges for all access to data/information.

4.5.4 Guidelines
(i) Applications and systems shall ensure that users change the initial/default passwords at their first log in.

(ii) Passwords shall not be included in log on scripts or other automated log on processes.

(iii) Access to systems and data shall be protected by passwords. Only authorised persons will be given user accounts and passwords for access. This access is restricted to the user requirements appropriate to his or her job duties.

(iv) The ICT Department shall be responsible for the administration of access controls to the WRTI ICT systems and resources and shall process additions, deletions and changes upon receipt of a request from the user's supervisor.

(v) The ICT Department shall maintain a list of administrator's passwords and keep this documentation in a secure area.

(vi) Access to accounts and passwords shall be protected by each user of systems and shall not be written down.

(vii) Users shall be required to use passwords that comply to the following guidelines:

(a) Passwords to accounts accessing or holding critical data/information shall be changed regularly and set to expire every ninety (90) days.

(b) Passwords to accounts accessing or holding critical data shall not be reused every twelve (12) months.

(c) Users shall not disclose passwords to others. Password shall be changed if the user suspects that it is known to others or discovers a security breach.

(d) All passwords shall be strong, that is, incorporate capital letters, special characters, digits and be at least eight (8) characters in total e.g. (P@ssw0rd).

(e) Passwords should not be simple and should not contain general information of the user such as anniversary dates or names of close family members or birthdates.

(f) The system shall automatically log off a user after three (3) unsuccessful login attempts when login to the systems portal.

NB: ICT Department shall ensure strict compliance to these requirements.

(viii) All users shall be responsible for all transactions made with their user ID and password.

(ix) Automatic Log Offs - Systems should automatically log out and terminate idle sessions after three (3) minutes.

(x) Screen Locks – Users shall password-protect their screensavers so that in case they have to leave their desk/office unattended for a short period of time, the screen will automatically be locked until a password is entered.

(xi) The ICT Head shall be notified by Human Resource Directorate when a user is transferred/dismissed/retires/resigns/on leave so that their user access can be revoked.

(xii) Wi-Fi passwords shall be changed after every ninety (90) days. Users shall NOT download, install, or run security programmes or utilities that reveal or exploit weaknesses in the security of the system.

4.6 Antivirus Management

4.6.1 Purpose

To protect the Institute's ICT resources from attacks by malicious software such as computer viruses, worms, Trojan horses, spyware, root kits and botnet.

It is important to note that computer viruses are much easier to prevent than to cure. Defences against computer viruses include; protection against unauthorised to computer systems, using only trusted sources for data and programmes, and maintaining virus-scanning software.

4.6.2 Scope

This policy applies to all ICT resources and staff of the Institute in regards to cyber security.

4.6.3 Policy

The Institute shall apply a dual anti-virus policy such that where there is connectivity, it will install a corporate antivirus and areas where there is no connectivity, single user antivirus shall be installed.

Any new computer or laptop shall be installed with the preferred antivirus software; and Any virus-infected computer shall be removed from the network until it is certified as being virus free.

4.6.4 Guidelines

The following guidelines are to assist in the prevention of virus attacks:

A. The ICT Department shall:

(i) Install and maintain appropriate licensed antivirus software on all computing devices and shall be configured to perform daily full-system and on-access scans.

(ii) Ensure regular updates and upgrades of the antivirus.

(iii) Respond to all virus attacks, eliminate any virus detected and document each incident and inform the users of infected computers of the action taken immediately.
(iv) Update regularly antivirus software on standalone devices.
(v) Ensure that antivirus is enabled at all times.

B. All Users Shall:

(i) Not introduce a computer virus into computing devices/network
(ii) Not load removable storage of unknown origin into Institute computing devices or network
(iii) Not download files/attachments from unknown or suspicious sources.
(iv) Scan removable media for viruses before being accessed.
(v) Immediately shut down the workstation and inform the ICT Department if they suspect that their workstation has been infected by a virus.
(vi) Neither open nor forward attachments/files to an email from an unknown, suspicious or untrusted source. These attachments shall be deleted immediately, and deleted again by emptying the recycle bin.
(vii) Avoid direct disk sharing with read/write access unless absolutely necessary.
(viii) Regularly update the antivirus software.

4.7 Backup and Recovery

4.7.1 Purpose

This policy is designed to protect data against loss and recover it in the event of an equipment failure, data loss, intentional or unintentional destruction of data, or disaster.

4.7.2 Scope

This policy applies to all core business data and systems, staff of the Instiute, and external service providers who may be responsible for the installation, support and security of data and information.

4.7.3 Policy

All Institutes' systems data shall be backed up and securely stored on site and off site.

4.7.4 Guidelines

(i) The ICT Department shall ensure that backup and recovery procedures for each system are documented and periodically reviewed.
(ii) Secure backups shall be taken on external media and may incorporate data encryption.
(iii) Backups shall be stored on site and off site securely.
(iv) Backups shall be protected using secure fireproof safe cabinets.
(v) Physical access controls shall be implemented at offsite backup storage and these locations shall meet or exceed the physical access controls of the source

systems. Additionally, backup media shall be protected in accordance with the highest sensitivity level of information stored.

(vi) A process shall be implemented to verify the success of the backups.

(vii) At least three generations of backup data shall be retained for important business data, software and applications. System Administrators shall establish and formally document an appropriate schedule for full and incremental backups.

(viii) Backups shall be periodically tested to ensure that they are recoverable.

(ix) Authorised staff access lists to offsite backup storage shall be reviewed annually or when an authorised individual leaves the Institute or Department.

(x) Procedures between the Institute and the offsite backup storage administration shall be reviewed annually.

(xi) Backup tapes/storage shall have the following minimum identification criteria by either labels and/or a bar-coding system:

(a) System name

(b) Creation date

(c) Sensitivity classification

(d) Retention regulations

(e) Contact information

(xii) System codes, configurations data, installations kits shall be part of data to be backed up and stored both onsite and offsite.

(xiii) All ICT systems delivered to the Institute shall have backup components.

(xiv) The ICT Department shall be responsible for:

(a) performing and verifying backups for core systems;

(b) checking that they have been successfully completed;

(c) recording the information on the backup register;

(d) ensuring that the backups are stored securely;

(e) Ensuring that the backup media are properly labelled; and

(f) Advising the Institute on requirements for backup.

4.8 Incident Reporting

4.8.1 Purpose

To ensure that incidents that involves ICT resources are reported to relevant authorities.

4.8.2 Scope

This policy applies to all Institute's ICT resources

4.8.3 Policy

All ICT related incidents shall be reported to the assigned duty officers/Supervisor/ Department/Directorate Heads or other officers as shall be advised by the Institute.

4.8.4 Guidelines

All incidences related to ICT resources shall be reported as:

(i) Incidents of theft, attempted theft and malicious physical damage shall be reported to the Head of the directorate affected, administration and ICT Head.

(ii) Incidents of data security breaches shall be reported to the ICT Head who shall in turn undertake appropriate action to mitigate or correct the incident and advice the management.

(iii) Incidents that disrupt normal functioning of ICT infrastructure for example system failure, and power disruption. within the Institute, shall be reported to Head of ICT for appropriate action.

4.9 Bring Your Own Device (BYOD)

4.9.1 Purpose

Bring-Your-Own-Device policy govern the Insttiutes' ICT department's level of support for employee-owned PCs, smartphones, tablets and those of any other authorised third party's accessing Institute's resources.

4.9.2 Scope

This policy applies to all WRTI staff and any authorised third party accessing the Institute's resources through BYOD.

4.9.3 Policy

(i) Employees who prefer to use their personally-owned ICT equipment for work purposes shall secure Institute data to the same extent as on Institute's ICT equipment, and shall not introduce unacceptable risks (such as malware) onto the corporate networks by failing to secure their own equipment

(ii) The employee shall assume full liability for risks including, but not limited to, the partial or complete loss of Institute and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

(iii) BYOD users shall use appropriate types of user authentication approved by ICT Head on Information Security, such as user IDs, passwords and authentication devices.

(iv) The use of foreign devices (BYOD) in the WRTI networks without the consent of the Head ICT is strictly prohibited.

4.9.4 Guidelines

(i) The Institute shall implement network access control (NAC) that will help in management of BYOD and IoT.

(ii) BYOD shall have no sensitive or confidential data/information and information system stored or installed in them.

(iii) The Institute has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the device.

(iv) The Institute has the right to seize and forensically examine any device within the Institute premises believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

(v) Suitable antivirus software shall be properly installed and running on all devices.

(vi) Device users shall ensure that valuable corporate data created or modified on the devices are backed up regularly, preferably by connecting to the corporate network and synchronizing the data between the device and a network drive or on removable media stored securely.

(vii) Any device used to access, store or process sensitive information shall encrypt data transferred over the network (e.g., using SSL or a VPN)

(viii) Device users are advised to keep their personal data separate from Institute's data.

(ix) Device owners shall not infringe other people's privacy rights.

ANNEX 5 : NETWORK MANAGEMENT

5.1.1 Purpose

To centrally and strategically coordinate network infrastructure planning and implementation.

5.1.2 Scope

The policy covers all network infrastructures such as Local Area Networks, Wide Area Networks and Wireless Networks; active devices such as firewalls, switches, routers, DTUs; cabling, bandwidth, internet**,** access points, IP Phones, Landline and controllers.

5.1.3 Policy

(i) Network infrastructure shall be centrally planned, managed and maintained by the ICT Department.

(ii) All network infrastructures shall incorporate firewalls, VLANs, NAT, encryptions, VPNs, intrusion detection systems, intrusion prevention systems and Network Management System, Network Admission Control among others.

(iii) VPN access is controlled using username and password authentication as is contained in WRTI's active directory.

(iv) ICT Department shall maintain network infrastructure designs, architectures, installations, configurations and documentations.

5.2 Internet and Email

5.2.1 Purpose

To provide secure access to internet and email services in the Institute for effective and secure communication.

5.2.2 Scope

This policy applies to all users who use internet and email services of the Institute.

5.2.3 Policy

Internet

(i) The ICT Department shall ensure that internet services are available to Institute's offices.

(ii) The ICT Department shall put in place mechanisms to restrict access to unauthorised and restricted sites.

(iii) Public internet access shall not be enabled on computing devices providing core business application.

Email

(i) The Institute shall provide electronic mail accounts to its staff for use to conduct official business.

(ii) All official electronic communications shall be done through official e-mail via the two registered domains; **wrti.go.ke and wrti.ac.ke.**

(iii) The ICT Department shall put measures in place to protect the e-mail system against misuse by staff.

(iv) The Institute shall inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfil the Institute's obligations.

(v) The Institute shall have a standard email disclaimer which users shall not remove or change when sending email messages.

DISCLAIMER: All the information contained in this email message is strictly confidential and may be legally privileged. Such information is intended exclusively for the use of the designated recipient(s). Any disclosure, copying or distribution of all or part of the information contained herein or other use of or the taking of any action in reliance upon this information by third parties is prohibited and may be unlawful. Although WRTI has taken reasonable precautions to ensure no viruses are present in this email, WRTI cannot accept responsibility for any loss or damage arising from the use of this email or attachments. If you have received this email message in error please delete it immediately and notify the institute through email wrti@wrti.go.ke

(vi) The ICT Department shall ensure that the users' emails are retained for as long as they are Institute's employees.

5.2.4 Guidelines

(i) The Head of HR Directorate shall forward names of officers to ICT Department who have joined/left the Institute for the purpose of creating or deactivating e-mail accounts.

(ii) Email addresses shall have the format "initial of firstname|lastname@wrti.go.ke|wrti.ac.ke" where two or more employees share the same first and last name, use the Last and the First name approach.

(iii) The ICT Department shall be responsible for creating the user accounts/emails of all the Institute's employees upon receiving formal request from HR.

(iv) The Institute's staff shall be required to use official email addresses for official communications at all times.

(v) Users who use the Institutes' internet services shall:

(a) Ensure that Internet is used in an effective, ethical, and lawful manner.

(b) Not use the Internet for purposes that are illegal, unethical, harmful to Institute or non-productive.

(c) Be responsible for the content of all text, audio, or images they place or send over the Internet.

(d) Not transmit copyrighted materials without permission from the copyright owner.

(e) Abide by all applicable policies dealing with security and confidentiality of records.

(f) Run virus scans on any attachments received through the internet.

(g) Be responsible for downloaded files or programmes. In case of doubt, users should contact the ICT Department.

(h) Not click on suspicious links, emails, documents from unknown sources. To ensure that all Institute employees are accorded the necessary ICT support while using ICT resources.

ANNEX 6.0: ICT SERVICE MANAGEMENT

6.1 User Support

6.1.1 Purpose

This provides guidelines on services provided by the ICT Department in the Institute with an aim of accelerating expeditious delivery of the mandate. These services include but not limited to internet provision, e-mail, hardware support, IP telephony, training, system and software development and support and advisory on emerging ICT Technologies.

6.1.2 Scope

This applies to all Institute employees.

6.1.3 Policy

(i) The ICT Department shall provide quality support to all users as per the ICT Department user support procedures.

(ii) ICT Department shall document all ICT support requests.

6.1.4 Guidelines

(i) Users shall immediately contact the ICT Department when they have ICT related issues.

(ii) The ICT Department shall be committed to offer ICT related support as stipulated by ICT service charter and process and procedures manual.

6.2 Shared Services

6.2.1 Purpose

To facilitate the sharing of services for cost effectiveness and interoperability.
The implementation of this policy will promote the availability, integrity and confidentiality of the Institute's ICT systems.

6.2.2 Scope

The policy shall cover resources that can be shared such as network infrastructure, Printers, Photocopiers, system applications, database and software licensing for purposes of maximizing the use of ICT resources.

6.2.3 Policy

(i) The Institute shall identify, facilitate and consolidate all services that can be shared.

(ii) All users shall share physical infrastructure such as computers, network infrastructure, printers, photocopiers and scanners.

6.2.4 Guidelines

(i) The ICT Department shall ensure that shared resources such as printers/copiers shall be accessed through authentication/authorisation.

(ii) Users/directorates or departments who wish to use the shared resources shall be authorised by ICT Department through writing.

(iii) The ICT Department shall deactivate users once they exit the Institute.

6.3 Service Charter

6.3.1 Purpose

To ensure that ICT Services are delivered effectively and efficiently.

6.3.2 Scope

This applies to all Institute employees.

6.3.3 Policy

There shall be an ICT Service Charter that shall give guidelines on services provided by the ICT Department to ensure that the Institute's employees are empowered to achieve operational efficiency in the performance of their duties.

6.3.4 Guidelines

(i) The ICT Department shall Document ICT Services.
(ii) The ICT Department shall adhere to the ICT service charter.
(iii) ICT Department shall review the ICT Service charter after every three years.
(iv) ICT service charter shall be displayed at common areas.
(v) ICT Service charter shall display the timelines and cost implications if any.

6.4 Documentation

6.4.1 Purpose

To ensure that all documentation for ICT resources is well-kept for reference and continuity purposes.

6.4.2 Scope

The policy shall cover all documentation in the Institute that relates to ICT systems and resources. The documentation includes among others:

(i) Service Level Agreement;

(ii) Contracts;
(iii) Networks designs, architecture and configurations;
(iv) Systems passwords;
(v) Project documentation;
(vi) inspection and Acceptance reports;
(vii) System audit reports;
(viii) User requirements and technical specifications;
(ix) User manual;

(x) Technical manual;
(xi) Installation and recoverable disks;
(xii) Feasibility study report; and
(xiii) Systems design report.

6.4.3 Policy
The ICT Department shall ensure ICT System/resources are documented and records stored ready to be availed when required. Vendors/Contractors shall deliver all ICT resources/systems with accompanying documentation.

6.4.4 Guidelines
(i) Monitoring and Evaluation teams to be appointed by the CEO/ Secretary to perform regular checks.

(ii) The ICT Department and SCMD shall be responsible and have custody of the documents indicated above.

(iii) All contractors where applicable shall provide documentation as indicated in the scope.

(iv) Documentation shall be stored both in hard or soft copy.

6.5 ICT Processes, Procedures and Manuals
6.5.1 Purpose
To provide general standard guidelines in the use of ICT services and resources.

6.5.2 Scope
This policy shall cover ICT processes and procedures for effective and efficient provision of ICT services to the Institute.

6.5.3 Policy
The ICT Department shall document processes and procedures manual.

6.5.4 Guidelines
The ICT Department shall—

(a) develop ICT processes and procedures;

(b) adhere to the ICT processes and procedures; and

(c) review the processes and procedures manual after every three years in accordance with COBIT 5 standards.

6.6 Technological Change Management
6.6.1 Purpose
The purpose of this policy is to establish a standard for technological change management. Change can disrupt service provision and therefore needs to be managed in a structured manner to ensure seamless transition.

6.6.2 Scope
The scope of this policy includes changes in ICT technologies, personnel and stakeholders.

6.6.3 Policy
All changes to configurations, systems, applications or equipment that could potentially affect the work of more than one person should follow the appropriate ICT Technological change management procedures to minimize adverse impacts of the changes to operations and the users of ICT Services.

6.6.4 Guidelines
(i) All changes require a Request for Change (RFC) shall be submitted by an authorised person to initiate the change. All RFCs will be classified based on category and urgency and the procedures for change management appropriate to the classification that should be followed.

(ii) Changes should be initiated by an authorised person and contain enough information to enable evaluation of the benefits and the risks associated with the change.

(iii) All Technological change management procedures should include the following activities:

(a) **Change Classification:** Each change should be classified according to the category of change requested and the urgency of the request. This will be used to determine the procedures that are to be followed.

(b) The evaluation will take into consideration the feasibility; human and physical resource requirements and costs; impact on the services provided to internal and external customers during the change; impact on services provided following the change; information security and risks.

(c) An authorised officer for the functional area should authorize the change based on the recommendation of the evaluation.

(d) The change should be scheduled at a time that will minimize disruption to services given the urgency of the request.

(e) Notification on the time, duration and services that could potentially be affected should be sent to all users affected by the change.

(f) A roll-back plan should be developed and implemented before the change is carried out. Where required by the procedures, the change should be tested successfully in a test environment before it is implemented.

(g) Users should be notified on the results of the change once complete.

(h) Users shall be taken through formal training on the new operational processes impacted by the change.

6.7 ICT Project Management

6.7.1 Purpose

To ensure that there is common and consistent application of formal project management methodology, principles and practice in the Institute.

6.7.2 Scope

This Policy Covers All ICT projects that shall be undertaken by the Institute.

6.7.3 Policy

All ICT related projects shall be implemented in line with the objectives of promoting E-Governance.

6.7.4 Guidelines

(a) The Director/CEO shall constitute an implementation team to oversee each ICT project.

(b) Implementation of any ICT project shall be done by a project implementation committee headed by a Project Manager who shall report to the committee.

(c) The Institute shall institute an inspection, evaluation, testing and acceptance committee to ensure quality of the project.

(d) All projects shall adhere to a project management methodology that will be prescribed by the ICT Head in liaison with the user Directorate/Department.

(e) All international contracted firms for the projects shall have a qualified local company that will provide support services to the project according to Public Procurement and Disposal Act.

(f) After completion of each project, a formal post-project review shall be undertaken by the Institute and the contracted firm to assess the following:

(i) Overall success;

(ii) scope management;

(iii) quality of deliverables;

(iv) key accomplishments;

(v) Problem areas and business process best practice established for continuous improvement; and

(vi) Sign-offs.

ANNEX 7: ICT BUSINESS CONTINUITY

7.1.1 Purpose

The purpose of this policy provision is to identify and establish processes, procedures and good working practices for the backup and timely recovery of the Institute's information and data existing in both electronic and physical form.

This provision aims to preserve the confidentiality, Integrity, and availability of WRTI Data and information for business continuity.

7.1.2 Scope

The scope of this policy provision extends to the back-up of all important information and data regardless of the form it takes - including the recovery of IT systems and supporting infrastructure.

This policy provision addresses risks, backup, business continuity and restore aspects of WRTI data and Information. All WRTI staff, contractors, service providers and consultants who process and/or store board data shall comply with this provision.

7.1.3 Guidelines

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practice.

The following guidelines will help ensure the Institute's information and data is backed up and restored securely in the most efficient manner possible:

(a) The WRTI Board shall provide resources for on premises and off-site backup.

(b) The WRTI Board shall identify and evaluate ICT risks and provide mitigation measures.

(c) The WRTI Board will ensure thorough and periodic review of all ICT related risks is undertaken, a dedicated ICT risk management mechanism needs shall be established.

(d) The ICT Department shall ensure full or differential backup is done in line with WRTI ISO quality systems procedure with Accurate and complete records of the backup copies and documented restoration procedures produced.

(e) Backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site

(f) The backups shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

(g) The WRTI staff are required to back up their data on the Corporate cloud platform in consultation with ICT department.

(h) The WRTI Board shall ensure adequate backup facilities are provided.

(i) The ICT Department shall develop a Disaster recovery plan to enable business continuity.

(j) Backup media shall be regularly tested to ensure that it can be relied upon for emergency use when necessary; this shall be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data shall be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss.

(k) In situations where confidentiality is of importance, backups shall be protected by means of encryption.

(l) Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

(m) WRTI shall optimize data processes, access, storage and management in line with ICT strategic plan 2024-2028.

7.1.4 ICT Systems/Data Backups

(a) The Institute's IT administrators shall be responsible for providing system support and data backup tasks and shall ensure that adequate backup and system recovery practices, processes and procedures are followed in line with the Institute's Disaster Recovery Procedures and data retention policies.

(b) All IT backup and recovery procedures shall be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery.

(c) All data, operating systems/domain infrastructure state data and supporting system configuration files shall be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration.

(d) All backup media shall be encrypted and appropriately labeled with date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should be kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster.

(e) There shall be a records system which shall be maintained to record all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc…) including any failures or other issues relating to the backup job.

(f) Copies of backup media shall be removed from devices as soon as possible when a backup or restore has been completed.

(g) Backup media which is retained on-site prior to being sent for storage at a remote location shall be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised.

(h) Access to the on-site backup location and storage safe shall be restricted to authorised personnel only.

(i) All backups identified for long term storage shall be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media.

(j) Backup media shall be protected in accordance with the appropriate data protection and media handling procedures.

(k) Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by the Institute's ICT systems. Where this may not be possible, photocopies of paper files shall be made and stored in a secure storage location.

(l) Regular tests shall be carried out to establish the effectiveness of the Institute's backup and restore procedures by restoring data/software from backup copies and analyzing the results.

(m) The ICT Support should notify the Head ICT when backups fail –providing information such as the backup job detail and reasons (if applicable) for the failure. A record shall be maintained, detailing the backup job failure including any actions taken.

(n) Backup data/media no longer required shall be clearly marked and recorded for secure disposal and with due environmental consideration (Waste, Electrical and Electronic Equipment - WEEE Directive).

7.1.5 User Responsibilities

(i) The Institute staff shall ensure Institute's data is securely maintained and is available for backup.

(ii) The Institute staff shall not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorized software which require the ‗caching' of files locally in order to function). Instead, Users shall save data (files) on their allocated areas – this could be an area within the EDRM system, a mapped drive or network shared folder the User has access to. Data (files) which are stored ―locally‖ will NOT be backed up and will therefore be at risk of exposure, damage, corruption or loss.

(iii) Where the Institute's network becomes unavailable for whatever reason, and data or work is at risk of being lost, users have no option but to save the data (files) locally (i.e. on the computer being used) or on approved media storage such as a Institute owned encrypted Data stick (USB storage). Once the Corporate Network

becomes available again, data (files) should be immediately transferred to the corporate network (Intranet)in order for it to be backed up safely and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored.

(iv) Authorized encrypted USB data sticks issued by the Institute should be used and any data stored shall be for temporary purposes. All sensitive, business and personal identifiable information should be removed from the USB data stick and moved to an appropriate Institute data network location as soon as possible in order to ensure the data is made available to the Institute and can be successfully backed up.

(v) Mobile phones should not be used to store sensitive, business or personal identifiable information. In the event of unforeseen or unavoidable situations leading to important data being stored on mobile phones, the data shall be stored to a suitable Institute network location and removed from the phone as soon as possible.

7.1.6 Data Restores

The Institute shall establish backup and restore routines. Data (file) restores should be carried out by the Server Support Team who will endeavour to restore files from a date specified by the user or from the nearest backed up date.

(a) IT Users shall request data (files) to be restored by contacting the IT Service Desk.
(b) Only files which the user is authorised to access will be provided from the restore.
(c) The IT Service Desk will need to verify that the User has permission and/or authorisation to view or obtain restored copies of file/s and/or folder/s.
(d) Users requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:
    (i) The reason for the restore
    (ii) The name of file/s and/or folder/s to be restored
    (iii) Original location of file/s and/or folder/s - the Service Desk will provide guidance to the User on how to find this out
    (iv) Date, day or time of deletion/corruption or nearest approximation
    (v) The last date, day or time which the User recalls the data (files) being intact and accessed/used successfully

(e) All backup and recovery (restore) procedures shall be documented and made available to Server Room personnel responsible for carrying out data (file) restores.
(f) Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing or other unforeseen

circumstance should be made under the supervision of the Server Support Team via Institute's IT Service Desk .

(g) Personnel accessing backup media for the purpose of a restore shall ensure that any media used is returned to a secure location when no longer required (applies to media from both Onsite and remote storage locations) .

(h) A log shall be maintained to record the use of backup media whenever it has been requested and/or used from secure storage

7.1.7 Cloud Computing

The Institute shall adopt the following cloud computing frameworks:

(i) Software as a Service (SaaS)
(ii) Platform as a Service (PaaS)
(iii) Infrastructure as a Service (IaaS)

7.1.7 1 Cloud computing security

WRTI shall adopt the following Cloud Computing Security approaches:

(i) Identity and Access Management (IAM)
(ii) Data Loss Prevention (DLP)
(iii) Security Information and Event Management (SIEM)
(iv) Business Continuity and Disaster Recovery (BCDR)

7.1.7 2 Cloud Computing Performance

WRTI shall use the following SLA metrics to measure cloud computing performance:

(a) **Response time:** The amount of time it takes for a request to be processed by the cloud and returned to the user.

(b) **Throughput:** The data transfer rate between the user and the cloud.

(c) **Scalability:** The ability of the cloud to handle an increasing workload without a significant decrease in performance.

(d) **Availability:** The percentage of time that the cloud service is accessible and functioning correctly.

(e) **Reliability:** The ability of the cloud to perform consistently and predictably over time.

(f) **Security:** The measures put in place to protect the data and applications hosted on the cloud.

(g) **Help Desks Support:** Timeliness of Vendor response to queries and support.

To optimise cloud computing performance, WRTI shall choose the right cloud provider, monitor performance regularly, and make any necessary adjustments to improve performance.

Cloud Computing Integration

(i) WRTI shall based on the needs of the Institute select the right cloud services and integration platforms to successfully integrate cloud computing services.

(ii) WRTI shall carefully plan and manage the integration process, including testing and monitoring the integration to ensure it works as intended.

(iii) The Institute shall ensure its cloud integration strategy includes robust security and compliance measures to protect sensitive data and comply with relevant regulations.

Cloud computing requirements.

There are essential requirements to be met when implementing cloud computing. Below are some of the critical requirements that WRTI shall adopt:

(i) Reliable Internet connection—Cloud computing services rely heavily on Internet connectivity to access and exchange data. Therefore, a reliable and stable internet connection is essential for seamless access to cloud services.

(ii) Scalable infrastructure—Cloud computing services require a robust and scalable infrastructure to meet changing business demands. WRTI shall ensure it has the infrastructure to support cloud-based workloads, including sufficient storage, memory, and processing power.

(iii) Cloud Service Provider (CSP) selection- WRTI shall select a reputable and reliable cloud service provider that meets the Institute's operations requirements, including compliance, security and availability. CSP offers a range of cloud services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

(iv) Cloud Security - Cloud computing requires a robust security strategy to protect sensitive data and applications. WRTI shall implement strong security measures, including data encryption, access controls and intrusion detection and prevention systems.

(v) Cloud governance – WRTI shall establish policies and procedures to govern cloud usage, including data management, compliance and risk management. This shall ensure that the Institute complies with legal and regulatory requirements and mitigates risks associated with cloud usage.

(vi) Cloud Migration Plan— WRTI shall have a well-defined plan for Migrating its existing ICT infrastructure, identifying candidates, and defining migration strategies.

By meeting these requirements, WRTI can successfully implement cloud computing and leverage its benefits, including improved scalability, flexibility and cost effectiveness.

ANNEX 8: ICT HEALTH AND SAFETY

8.1.1 Purpose

This policy will ensure that members of staff are using WRTI ICT resources in a healthy and safe manner.

8.1.2 Scope

This policy applies to all staff using the WRTI ICT resources.

8.1.3 Policy

The Institute shall:

(a) provide a healthy and safe environment for staff to use ICT resources;

(b) ensure that there is a system in place for regular health and safety checks (that will include visual checks of plugs, leads and other electrical equipment); and

(c) ensure that guidelines issued under the Occupational Safety and Health Act (Cap. 236A) are observed.

8.1.4 Guidelines

I. **Comfort**

(i) The Institute shall provide the recommended working tools for ICT equipment.

(ii) Users should be provided with comfortable work stations. While sitting, users shall be able to adjust their position in relation to the equipment as appropriate. (Health ergonomics).

(iii) Users should change posture frequently and take frequent thirty minutes break away from the computer to stretch their limbs and rest their eyes.

Desks and workstations

There should be enough space around a workstation for paper, books and other working tools. Desk design should take care of cable management. Gangways and emergency exits shall be kept clear.

Sitting

When using ICT equipment, users need to sit at the recommended height (with the eye level at the top of the screen).

Monitors

Monitors should tilt and swivel to suit the requirements of individual users. The top of the screen should be roughly at eye level. Screens should be positioned to reduce reflection and glare from lights and windows and should be adjustable for brightness and contrast as the lighting changes throughout the day. Clean screens give better visibility and reduce glare. Screen distortion may occur if speakers are placed too close to the monitor, so it is advisable to position them about 30cm away.

Keyboards

Users should have the option of using the keyboard flat or tilted. It is important for users to develop a good keyboard technique; do not bend hands up at the wrist when typing, keep a soft touch on the keys and do not over-stretch your fingers. Straining may cause Repetitive Strain Injury (RSI - upper limb disorders including pains in the neck, arms, elbows, wrists, hands and fingers), a painful condition which has the potential to cause irreversible problems.

Screen projectors

When using a projector, make sure that equipment is monitored at all times during the projector's operation. One should never stare directly into the beam of the projector.

Personal Safety

Users should be cautious when using specialized equipment such as shredders, Printers, scanners, and photocopiers since fast-moving parts can trap clothing, jewellery and hair and may cause harm to them.

Electrical Safety

All electrical equipment should be maintained regularly. Technical repairs should be left to the experts. The location of electrical equipment depends on the length of cables and the availability of sockets. It is essential that the location of the equipment does not increase the risk of danger to equipment or users.

Mobile Equipment

The risk of lifting heavy or bulky equipment shall be assessed and trolleys should be used where appropriate. It is advisable to push a trolley rather than pull it. When using mobile equipment such as projectors, they shall be anchored firmly when in use.

Hazardous substances

Risk assessment is necessary when using toners, printing ink and cleaning materials. Fluids used for cleaning and in some reprographic processes are flammable. They should not be used in confined spaces and adequate ventilation should be maintained.

ANNEX 9: PROHIBITITION, RESTRICTIONS AND PENALTIES

9.1 Prohibition and Restrictions

It is important for users to be aware of applicable laws and regulations when accessing or using data or systems that are internal or external to the Institute. Areas of consideration should include but not limited to copyright, trademarks, patent, privacy, wiretap confidentiality and communication laws and regulations. Use of computing resources to violate laws or regulations represents violation of this ICT Policy.

The following activities are generally prohibited or restricted. Certain individuals may be exempted from these rules in order to perform their required responsibilities (e.g., System administrators and Network administrators are authorised to actively monitor network traffic and respond in a disruptive manner to mitigate a detected threat). Employees are not authorised, under any circumstances, to actively engage in activities deemed illegal under applicable jurisdictions.

The list provided below is not comprehensive, but should be used as a baseline to help determine whether an action is permissible. Omission of an action from this list does not imply that it is an acceptable use. Any violations of these specific prohibitions may result in immediate disciplinary action.

9.2 Illegal Use

(i) Computing resources shall be used within the confines of the law.

(ii) Any use of computing resources to infringe intellectual property protections, such as copyrights, trademarks, patents or trade secrets, is prohibited.

(iii) Infringing acts may include, but are not limited to, unauthorised copying of copyrighted materials, use of a trademark without authorisation or exporting software, technical information, encryption or technology in violation of export control laws.

(iv) Any action, intentional or unintentional, that serves to copy or transmit protected materials without proper authorisation is an unacceptable use.

9.3 Threats or Harassment

Computing resources shall not be used to threaten, harass or harm others. Unauthorised use includes but is not limited to:

(i) Communication that is threatening, abusive, harassing, defamatory, libellous, deceptive, fraudulent, invasive of another's privacy, tortuous, or containing explicit or graphic descriptions or accounts of sexual acts (including but not limited to sexual language of a violent or threatening nature directed at another individual or group of individuals);

(ii) Communication that victimizes, harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, gender, sexual orientation, race, ethnicity, age, or disability; or

(iii) Any form of harassment via email, telephone, social media or instant messaging, whether through language, frequency, or size of messages;

9.4 Fraud Forgery or Impersonation

(i) Any use of computing resources to commit fraud, forgery or impersonation is strictly prohibited.

(ii) All users shall truthfully and accurately represent their identity at all times.

(iii) Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited.

(iv) Any attempt to impersonate any person by using forged headers, including email header information, or other identifying information is prohibited.

(v) Posting on public or private sites with the intention to hide employment status and employer details for fraudulent purposes, is prohibited.

9.5 Spam/Spim

(i) Creation, sending and forwarding of unsolicited advertising, junk or bulk email ("SPAM") or instant messages ("SPIM") are strictly prohibited, unless explicitly authorised as part of your normal job duties.

(ii) Undertaking any activities that facilitates unsolicited commercial emails or unsolicited bulk emails, whether or not those emails are commercial in nature, is prohibited.

(iii) Use of instant messaging facilities to accomplish the same is also prohibited.

9.6 Unauthorised Access

(i) Any access to systems or data that is not specifically authorised is prohibited.

(ii) Any circumvention of access controls, whether for accessing systems with or without authorisation, is also prohibited.

(iii) Users shall not access unauthorised sites by use of another person's identity i.e., Tailgating.

(iv) Users shall not circumvent authentication or security of any host, network or account.

9.7 Collection of Confidential Data

(i) Use of computing resources to collect confidential data, is prohibited.

(ii) Collection, or attempts to collect, personal information about third parties, without their knowledge or consent, is prohibited and may constitute a violation of Institutes' privacy policies and agreements.

(iii) The Institute has limited liability in cases where individuals act on their own accord and without proper authorisation.

(iv) Any attempts to collect confidential data without explicit and proper authorisation is prohibited and will be subject to severe disciplinary actions

9.8 Disrupting network services or access to data

(i) Rendering systems, networks, applications or data inaccessible or unusable due to an unauthorised disruption or corruption, is prohibited. Such prohibited acts may include, but are not limited to, ping floods, packet spoofing, executing denial of service or distributed denial of service attacks, forging routing information, corrupting data upon which an application or system relies, or removing or disabling a service, such as a process or application, on a host or network.

(ii) Port or security scanning without prior authorisation by operations security is strictly prohibited.

(iii) Using any automated tool, such as a program, script or command, to send any message with the intent to interfere with or disable terminal sessions is not acceptable.

9.9 Disclosure of Protected information

(i) Disclosing the Institute's confidential information is prohibited. Disclosures may include, but are not limited to, unique account names, account passwords or lists of employees, contractors, consultants, vendors or products.

(ii) All information shall be treated as confidential and protected unless labelled otherwise.

(iii) Information relating to email address, assigned desk phone number, fax number, mailing address or title shall not be deemed to be protected information.

9.10 Monitoring or Interception of Network Traffic

(i) Monitoring or intercepting any form of network traffic or data not intended for your own host is prohibited, unless authorised as part of your normal job duties.

(ii) Monitoring or intercepting network traffic may violate the privacy or confidentiality of the data being transmitted.

9.11 Introduction of Network Services or routing configurations

The introduction of routing patterns or network services that are inconsistent with established patterns or services and/or that may disrupt or interfere with the intended patterns or services are expressly prohibited.

Examples of unacceptable use include, but are not limited to, broadcasting routing information, providing Dynamic Host Control Protocol (DHCP) services in conflict with authorised services, or sending network messages designed to terminate network connections (such as TCP RST packets, or "sniping").

9.12 Release of Information regarding Security Incidents

(i) Authorisation to release information regarding security incidents involving the Institute is restricted solely to management and its assigned agents (i.e., legal counsel or public relations agents).

(ii) In the event of a security incident involving the Institute, individuals are not authorised to communicate news of such incidents to any outside party. It is solely the Institute's responsibility to appropriately notify public of security incidents in compliance with government regulations.

9.13 Penalties

An employee of the Institute shall accept the terms of this ICT Policy and agree to abide by its provisions. Failure to observe the ICT policy may result in disciplinary action by the Institute and/or legal action.

Action may be taken against any officer who contravenes the requirements of this policy as per the relevant law in Kenya.