KENYA FORESTRY RESEARCH INSTITUTE

Information and Communication Technology

Policy Guidelines
2018

DOCUMENT & VERSION REVISION HISTORY				
No	**DOCUMENT & Version, Release or Build Number**	**REVISION DATE**	**REVISION DESCRIPTION**	**REVISION TRACKING NOTES**
1	Information and Communication Technology Policy Guidelines 2014	30/6/2014	Document to be reviewed after three years or due to any other reasons as may be determined from time to time by Management	Version 1.0
2	Information and Communication Technology Policy Guidelines 2017	15/6/2018	Document to be reviewed after three years or due to any other reasons as may be determined from time to time by Management	Version 1.0

This policy was written for and produced by Kenya Forestry Research Institute (KEFRI)
P.O Box 20412 - 00200 Nairobi
Tel: +254-724-259781/2,
Wireless: +254-2010651/2
Email: info@kefri.org
Website: www.kefri.org

Abbreviations and Acronyms

BYOD	Bring Your Own Device
ERP	Enterprise Resource Planning
HICT	Head ICT
ICT	Information and communication Technology
KEFRI	Kenya Forestry Research Institute
LAN	Local Area Network
OPAC	Online public access catalogue
PC	Personal Computer
STI	Science, Technology and Innovation
UPS	Uninterruptible Power Supply
VLANS	Virtual Local Area Network
WAN	Wide Area Networks

Table of Contents

Abbreviations and Acronyms 3

Preamble 6

1. Introduction 7

1.1 Why ICT 7

1.2 Vision of ICT Policy 7

1.3 Mission of ICT Policy 7

1.4 Policy Objectives 7

1.5 Application and Scope 8

2. Roles and Responsibilities 8

2.1 Management 8

2.2 Head of ICT: 9

2.3 Heads of Departments/Divisions/Sections: 9

2.4 User Responsibilities 9

3. Key Policy Areas 9

3.1 ICT Usage 9

3.1.1 Acceptable Use 9

3.1.2 Unacceptable Use 10

3.1.3 Software and Hardware Usage Guidelines 10

3.1.4 Hardware Usage 11

3.1.5 Asset Administration 11

3.1.6 Restitution 11

3.1.7 Bring Your Own Device (BYOD) 11

3.1.8 Remote working policy 12

3.1.9 Usage tracking and Monitoring 13

3.10 Precautionary and Disciplinary Measures 14

4. Electronic Communications 14

4.1 Email 14

4.2 Internet Policy 15

4.3 Personal Blogs, Web content and social media platforms 15

4.4 Access with consent/ Access without consent 16

5. System Applications 17

5.1 General Configuration Guidelines 17

5.2 Website Policy 17

5.3 System Integration Policy 17

5.4 New Systems Changeover Policy 18

5.5 Digital Content/Repositories....18
6. Network Infrastructure....18
6.1 Accessibility....20
6.2 Infrastructure Policy....20
6.3 Power supply Policy....21
6.4 Wireless Networks....22
6.5 Virtual Private Networks (VPN)....23
7. ICT security policy....25
7.1 Physical Security....32
7.1.1 Required Physical Security....32
7.1.2 Computer Server Rooms....32
7.1.3 Access Control....33
7.2 Network and Information Security and Access Policy....33
7.3 Information Classification....33
7.4 Usage Monitoring, Privacy and Surveillance policy....34
7.5 Passwords and Access codes Policy....34
7.6 Virus protection policy....35
8. ICT acquisition, maintenance repair and disposal....36
9. ICT User support and training....38
10. Legal....39
11. ICT Data Backup, Disaster Recovery and Preparedness Policy....40
12. Enforcement, auditing and reporting....42
13. Revision....43
14. Reference....43
15. Approval....44

Preamble

The vision of KEFRI is to be a centre of excellence in forestry research for development. Guided by this vision, the Institute has strategically positioned itself:

- To enhance: Vision 2030 delivery; customer/stakeholder satisfaction and retention; linkage and partnership with stakeholders; and livelihoods.
- To increase forest technologies and innovations; enhance multi-sectoral and public-private sector research; enhance knowledge management and dissemination systems.

Information Communication and Technology (ICT) plays a vital role in achieving the Institute's vision and mission. The use of ICT in appropriate contexts can enhance research and information dissemination through the addition of different dimensions that were not previously available.

The ICT Section, on behalf of the Institute, has taken the mandate of developing an ICT policy to act as a guide in the effective use of ICT resources in the Institute.

Preparation of this policy has been necessitated by the rapidly changing technologies, not to mention the need to integrate the Institute ICT policy to be in line with the Kenyan National ICT Policy framework. ICT is always evolving and contributes immensely to economic, political, social, scientific and educational development in every society where it is deployed.

It is the existence and utilization of appropriate ICT policy that enables individuals, institutions, Institutes, nations, or regions to benefit from the developments propelled by the application of ICT.

The KEFRI ICT policy framework spells out the principles and goals intended to govern the accusation, development, implementation, adoption, monitoring, evaluation, application and of Information Communication and Technology (ICT) in Kenya Forestry Research Institute.

This ICT Policy document further seeks to provide guidelines for compliance, acceptable and secure use of ICT systems by both KEFRI employees and stakeholders.

1. Introduction

1.1 Why ICT

Information in the modern context is considered as a strategic resource parallel in importance to land, labour, capital, and entrepreneurship – the traditional economic resources which are vital inputs for national development at all levels. Without information, the very functioning of society would come to a standstill.

Reliable and efficient ICT systems are crucial to the operation of the Institute, given the frequency with which staff, researchers and administrators exchange information between research partners, programmes, divisions, sections and centers. ICT systems that can 'talk to' each other are needed and to which individuals can gain access, whether they are working within the Institute, a department or center, or outside the Institute.

Further, in an environment where there is increasing interdependencies and interdisciplinary work being carried out, ICT systems are needed that facilitate the sharing and exchange of ideas, information and knowledge.

1.2 Vision of ICT Policy

To provide support to KEFRI vision by application of up-to-date ICT Technologies

1.3 Mission of ICT Policy

To provide best ICT practices to enable KEFRI achieve its mission.

1.4 Policy Objectives

The objectives of this Policy are to,

- Promote the provision of accessible, universal, affordable, reliable, modern, secure and high quality levels of ICT facilities and services.
  To serve as a guideline for on ICT practice and procedures
- Provide clarity for users of the system regarding rights and privileges to use ICT Infrastructure
- Guide the handling of Institution's ICT Infrastructure and information within the Institute by ensuring compliance with applicable standards, statutes, regulations, and mandates for the management of ICT resources in line with the priorities of the Institute;

- Establish the Institute's strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, managed, and/or controlled by the Institute.

- Provide a framework for the management of ICT assets that shall ensure enhanced performance of business processes, improve decision making, and reduce the cost of running the ICT infrastructure;

- Uphold the integrity and image of the Institute through defined standards and guidelines for ensuring that the content of the KEFRI's websites, repositories and portals are accurate, consistent and up-to-date

1.5 Application and Scope

This policy shall be the reference document for any person accessing/developing/implementing and/or using ICT-based information and ICT resources owned, managed, supported or operated by, or on behalf of the Institute. It applies to all KEFRI staff; any other Institutes accessing services over KEFRI ICT resources; persons contracted to develop, repair or maintain KEFRI's ICT resources; and suppliers of outsourced ICT services. Adherence to this policy applies to all these and other relevant parties.

Information assets addressed by the policy include but not limited to, data, information systems, computers, network devices, as well as documents and verbally communicated information.

The document shall be effective from the date of approval.

2. Roles and Responsibilities

2.1 Management

Management will avail resources to purchase and license the required security hardware and software (security equipment, central anti-virus, firewalls, VPNs) and adequate staffing to manage infrastructure, train users and conduct routine security audit procedures to effectively implement this policy.

2.2 Head of ICT:

- Ensure coordination, implementation and compliance of the policy.
- Provide support and guidance to users in understanding their responsibilities with regard to the policy.
- Recommend /advise on the appropriate software to be acquired and installed

2.3 Heads of Departments/Divisions/Sections:

- Ensure that all users under their supervision are aware of this policy and comply with it.
- Ensure that breaches of this policy are reported to the management to be resolved in accordance with the laid down disciplinary procedures.
- Human Resources division to notify the ICT section whenever an employee leaves the Institute or transfers to another Departments/Divisions/Sections or there are changes in responsibility so that his/her access rights can be revoked or changed.

2.4 User Responsibilities

- Understand and adhere to the policy.
- Notify any breach of policy to the management.

3. Key Policy Areas

This policy will cover the following areas

3.1 ICT Usage

While KEFRI provides ICT facilities for use by staff and other stakeholders, the right to access and use such facilities shall be controlled by guidelines developed and shared with all users.

3.1.1 Acceptable Use

- Users of ICT Systems are expected to use them responsibly and securely in a manner that minimises the risk of detrimental impact to the Institute. That is, to comply with all applicable laws, other Institutional policies, and professional standards, personal courtesy and conduct.

- All information stored or transmitted through the Institute's ICT systems must conform to law and the Institutional policies regarding protection of intellectual property, including laws and policies regarding licensing, copyright, patents, and trademarks.

- The Institute's ICT systems should be used primarily for research and business purposes. Some incidental personal use of the Institute's ICT systems by staff is allowed as long as:
  a. It does not consume more than an insignificant amount of system resources;
  b. It does not interfere with your productivity or that of others;
  c. The activity is legal and in compliance with Institute's codes of conduct or policies;
  d. sensitive information or systems belonging to the Institute are not placed at risk of compromise;
  e. It does not pre-empt any research activity of the Institute.

3.1.2 Unacceptable Use

The Institute's ICT systems must not be used for:

- Unlawful, fraudulent or libellous activities;
- Commercial purposes not under the auspices of the Institute;
- Personal financial gain;
- political activities;
- engaging in any form of intelligence collection from the Institute's information assets;
- activities that put the reputation of the Institute or its employees at risk;
- activities that violate other Institutional policies or guidelines

3.1.3 Software and Hardware Usage Guidelines

3.1.3.1 Software Usage

KEFRI has acquired licenses of computer software from a variety of third party vendors. The purpose of this policy is to prevent copyright infringement and to ensure proper software asset management.

It is the obligation of KEFRI to respect and adhere to all computer software copyrights and the terms of all software licenses procured. It is also the obligation of KEFRI to manage its software assets and to ensure that Institute installs and uses only legal software on its PCs (including mobile devices) and servers.

Unauthorized duplication of software may subject users and/or Institute to both civil and criminal penalties. KEFRI will not permit any employee to use software in any manner inconsistent with the Manufacturer's applicable license agreement. The Institute shall acquire copy, distribute, transmit and use software in accordance with the terms and conditions of any license agreement accompanying a particular software product.

3.1.3.2 Acquisition of Software

All requests for software (System and application software) including purchase, installations and upgrades, must be submitted to the ICT Section as per the Institute's Quality Management System procedures. Software will be purchased only from reputable, authorized sellers.

3.1.4 Hardware Usage

Hardware devices and network systems purchased and provided by KEFRI are to be used only for creating, researching and processing business related materials. By using the Institute's hardware and network systems users assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable Institute policies. All hardware devices and network systems are to be used ethically, lawfully and appropriately at all times.

All requests for computing hardware devices must be submitted to the ICT section for review on adherence to standard hardware that best accommodates the desired request.
All specifications for purchase of Institute ICT hardware devices shall be centralized with the ICT Section to ensure that all equipment conforms to institution hardware standards.

3.1.5 Asset Administration

No alterations, upgrades or modifications should be made to hardware purchased by the Institute and provided to the employee, unless approved in writing by the ICT section. KEFRI retains ownership of all hardware and software provided to users.
Users should ensure the hardware devices provided by the Institute are protected from theft and physical damage using reasonable precautions.

3.1.6 Restitution

Should an employee fail to return Institute -provided equipment and software upon termination or at the request of the ICT section, the employee shall pay the Institute the book value of the ICT asset as determined by the Institute.

3.1.7 Bring Your Own Device (BYOD)

The Institute recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, on campus or while travelling. Such devices include but not limited to,

laptops, smart phones and tablets, and the practice is commonly known as 'Bring Your Own Device' or BYOD. The Institute is committed to supporting staff and stakeholders in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing the Institute provided services on BYOD.

The Institute must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

a. Familiarise themselves with their device and its security features so that they can ensure the safety of Institute information (as well as their own information)
b. Invoke the relevant security features
c. Maintain the device themselves ensuring it is regularly patched and upgraded
d. Ensure that the device is not used for any purpose that would be at odds with the Institute policies
e. Not violate clause 3.1.3 above

While Institute's ICT staff will always endeavour to assist colleagues wherever possible, the Institute cannot take responsibility for supporting devices it does not provide.

It should be noted that the Institute does reserve the right to:

a. Prevent access to a particular device from either the wired or wireless networks or both
b. Wipe corporate data from the device
c. Lock the device to prevent use
d. Prevent access from the device to the corporate network and its resources
e. Take all necessary and appropriate steps to retrieve information owned by the Institute

3.1.8 Remote working policy

Remote working is a work arrangement that permits an employee to conduct all or some of their work at an approved alternative worksite such as the home or in office space near to the employee's home.
Employees must ensure security of information and systems accessed through mobile and remote working arrangements are given due consideration.

The line manager will discuss and agree with the employee prior to commencing remote working, what equipment and IT requirements

will be needed to enable the individual to work effectively from home. The equipment will remain the property of the Institute at all times.

When you are working remotely you must:

a. Take reasonable care of the equipment;
b. Take all reasonable steps to minimize the risk of theft or damage to Institute's property whilst these items are away from Institute premises;
c. Use it only for work purposes and in accordance with any operating instructions as defined in the Institute Information Security Policy;
d. Comply with clause 3.1.3 above;
e. Return to the Institute, the equipment at the end of the Remote working arrangement.

3.1.9 Usage tracking and Monitoring

As a general definition, Usage tracking and Monitoring involves the use of software to track computer activities.
Monitoring may include tracking of network activities and security threats, as well as Internet usage, data entry, e-mail and other computer use by individual users. Monitoring is done by someone other than the user, and may be made known to the user or may be surreptitious. In either case, the user has no control over the monitoring activities and the data that is generated.

KEFRI may conduct monitoring as described in this document, and in additional notices that may be provided to you, subject to applicable laws and regulations. KEFRI's monitoring activities may include:

a. monitoring and logging of (1) traffic and usage data (such as routing, addressing, or signalling information, time and date stamps, sender and recipient details and file size) related to incoming, outgoing and internal electronic communications, including emails sent to and from KEFRI accounts, chats and instant messages on KEFRI approved channels for business use and any other data moving across the Systems (including internet traffic); and (2) Systems activity, including files or information accessed or downloaded from, or uploaded to Systems;
b. monitoring contents of (1) emails sent to and from KEFRI accounts; (2) chats and instant messages on KEFRI approved channels for business use; (3) faxes sent to or from KEFRI fax numbers; (4) text messages (SMS) sent to or from Systems; (5) files or information accessed or downloaded from, or uploaded to Systems; and (6) internet usage (including pages visited and searches made) (collectively, the "Content");

c. monitoring telephone calls to or from KEFRI work telephones as required or permitted by applicable laws and subject to any required notices;
d. capturing Workers' physical presence at KEFRI's facilities via for example access badges and video cameras, which record activities at exits, entrances, corridors, and other public areas; and logging hours worked if applicable to the Worker.

3.10 Precautionary and Disciplinary Measures

Any user who abuses the privilege of KEFRI-facilitated access to ICT systems and Infrastructure can be subject to disciplinary measures which may include the offender being denied access to computing facilities.

4. Electronic Communications

4.1 Email

Every employee of the Institute with email access is responsible for ensuring that the electronic mail ("e-mail") system is used properly and in accordance with this policy.

Official KEFRI e-mails are provided for to all staff on prefix @kefri.org. The format shall follow the convention shown below unless stated otherwise. {First name initial followed by lastname@kefri.org}. E-mail is recognized as official means of communication. E-Mail archiving regime shall also be maintained in line with government policy on disposal of government documents.

It is prohibited to use the Institute's Email system to;

a. Create or exchange offensive or obscene messages of any kind, including pornographic material.
b. Send e-mail that promotes discrimination, intolerance, and/or fear of others on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
c. Send e-mail that promotes party politics, and/or partisan views on political issues.
d. Send e-mail that contains a threatening or violent message.
e. Exchange proprietary information or other confidential information (including but not limited to financial reports, financial data, HR or personnel information, donor contract information) with anyone not affiliated with the Institute.
f. Create, forward, or exchange SPAM, chain letters, solicitations, or advertising.

g. Create, store, or exchange e-mail that violates material protected under copyright laws.
h. Distribute Institution's data to the Institute's suppliers or partners without proper authorization.
i. Alter a message from another user without their permission.
j. Forge headers or otherwise manipulate messages in order to disguise the origin of any content transmitted. Users shall not falsely state or misrepresent your identity.
k. Improperly using someone else's e-mail account as your own without their permission.
l. Avail our email system for use by third parties (including suppliers and partners)

4.2 Internet Policy

The Institute shall provide Internet services to staff for official use on research and collaboration for non-business purposes and restrict personal use to minimum limited to educational, knowledge and news sites.

KEFRI reserve the right on the content accessed and the users allowed to access Internet. This Policy expresses the Institute's view on access rights, use and conduct of all users.
Users shall not use or access the Internet Users will strictly avoid visiting non-business, offensive and unethical sites, which violate security policies.

The Institute reserves the right to restrict access of specific sites during working hours (e.g. Facebook, Twitter, YouTube etc.)

4.3 Personal Blogs, Web content and social media platforms

This part of the policy applies to personal blogs, web content and other social media platforms even if created, updated, modified or contributed to outside of working hours or when using personal ICT systems.

a. KEFRI recognizes that at your own private time you may wish to contribute to online forums, such as websites, blogs, and message boards, or you may take part in social media platforms or forums of a similar nature. For the avoidance of doubt, such as activities are expressly prohibited during work time or using institutional systems.

b. If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of KEFRI staff and/or you discuss your work or anything related to Institute or its mandate, customers or staff, KEFRI expects you, at all time, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with institutional policies and procedures. It

should be noted that simply revealing your name or visual image of yourself could be sufficient to identify you as an individual who works for KEFRI.

c. If a blog posting clearly identifies that you work for KEFRI and you express any idea or opinion then you should add a disclaimer such as 'these are my own personal views and not those of KEFRI'.

d. The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive)

   i. Revealing confidential information about KEFRI in a personal online posting.
   ii. This might include revealing information relating to KEFRI clients, research plans, policies, staff, financial information or internal discussions. Consult your supervisor if you are unclear about what might be confidential.
   iii. Using an anonymous email, personal blog or website to criticize or embarrass KEFRI, its clients or it staff. You should respect the corporate reputation of the Institute and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise a grievance using grievance procedure

If you think that something personal on your blog or website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role then this must be discussed with your supervisor

4.4 Access with consent/ Access without consent

This part of the policy strives to protect the privacy of employees', data (such as Electronic communications primarily consist of e-mail and attachments and Files Created on a Computer), except in situations where legal requirements take precedence.

If access to those electronic communications is required, the appropriate consent procedures must be followed.

Any review, whether limited to computer files for which no consent is required or including e-mail and attachments pursuant to authorized access, should be limited to the minimum necessary review in order to resolve the situation.

5. System Applications

5.1 General Configuration Guidelines

- Server Operating Systems shall be configured in line with approved ICT guidelines.
- Access to services shall be logged and protected through access-control methods.
- The most recent security patches shall be installed on the systems as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Antivirus software shall be installed and configured to update regularly.
- User access privileges on a server shall be allocated on "least possible required privilege" terms, just sufficient privilege for one to access or perform the desired function.
- Servers shall be physically located in an access-controlled environment.

5.2 Website Policy

It is the policy of KEFRI to disseminate information that is current, accurate, complete and consistent with Institute's policies. Information released via the Internet is subject to the same official Institute's policies for the release of information via other channels (such as printed documents).

Update the website frequently on current issues happening within the Institute with respective departments expected to forward information to the Information Office for vetting before the Web Masters upload the information to the website.
Hosting shall be outsourced to ensure availability of the website at all times.

5.3 System Integration Policy

KEFRI policy is to have all systems integrated for ease of data sharing and minimize on data duplication within its systems and inconsistency. Where possible all systems will be evaluated to check on common ground that will enable use of a single database for ease of data interchange amongst systems.

5.4 New Systems Changeover Policy

With increasing automation and modernization of KEFRI's processes for efficient service delivery, systems will be integrated and new systems developed. This necessitates the need for this changeover policy to allow the Institute, for smooth adoption of the systems with minimal disruption of services.
This policy proposes use of changeover strategies such as parallel runs, integration testing, and acceptance testing amongst others. It is the policy of KEFRI therefore that before any major system changeover, a changeover strategy

5.5 Digital Content/Repositories

KEFRI recognize that most of the information resources shall be in digital form as web resources/ electronic journals/repositories, accessible within the Institute or without. It is therefore the policy of KEFRI to continuously modernize its Infrastructure in order to facilitate provision of information resources in electronic and digital formats. Appropriate facilities shall be sourced in order to ensure all users have access to the materials held by KEFRI.

This policy recognizes that KEFRI will observe legal regime within the Kenyan laws and International laws governing intellectual property rights and copyrights of digital and electronic materials. It is observed that KEFRI will not be held responsible for any use or otherwise by its clients other than the purpose intended (research and information repository).
It is expected that KEFRI will continue with use of online public access catalog (OPAC) in the management of library resources, while providing link to subscribed local and international repositories.

6. Network Infrastructure

This policy describes the guidelines for the use and expansion of the Institute wired and wireless campus network. Use of the network, and growth and expansion of the network, must meet community expectations and provide consistent experience for the entire Institute community. Institute may prohibit or restrict network access for technical, regulatory compliance, legal, or policy considerations at any time.
Access Point: The electronic hardware that serve as a common connection point for devices in a Wireless Network. An Access Point acts as a network interface point that is used to extend LAN segments, using Radio Frequency signals instead of electrical signals on a wire for access by multiple users of the Wireless Network. Access Points are shared bandwidth devices and can be connected to the Wired Network.

Core Network Services: Include, but are not limited to: Windows Internet Naming Services (WINS); Domain Name System (DNS); Dynamic Host Configuration Protocol (DHCP); Internet Protocol addressing (IP address);

Media Access Control addressing (MAC); routing and switching; network connectivity; voice and data transmission; and Internet services.

Coverage: The geographical or building area where a baseline level of wireless connection service quality is provided or accessible, intentionally or unintentionally. In the case of a Wired Network, Coverage, for the purposes of this document, is defined as the local area network or network segment that is represented by the physical location of network drops or nodes on the network.

Domain Names:
A name that identifies one or more IP addresses, Domain Names are used in Uniform Resource Locators (URL's) to identify particular web pages. UTS is responsible for maintenance of oakland.edu administration on the Educause web site registration service.

Firewall(s): A technical network implementation that protects computers on a specific network from intentional, accidental, hostile or unauthorized intrusion. Several firewall implementations may exist at any time, collectively referred to as Firewalls.

Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS): Devices, software applications, or combination device/software solutions that monitor network or system activities for malicious actions, attempted perimeter violations, or policy violations, and may log, report, issue alarms, or take automated actions.

Network Components: The individual devices such as drops, ports, hubs, routers and switches that support the technical implementation, connectivity, and the operation of the network.

Network Infrastructure: The inter-building and intra-building voice, data and video wired or wireless transport systems, and the electronic components and communication Protocols used to transport signals over the systems. In its simplest form, a network connects two or more computers together.

Network Resources: Systems, servers, file sharing and storage, printing and other items attached to the network that can be utilized through connection to the network.

Protocols: The defined format for communications transmission among devices, including the rules or sets of rules that create a communications and error handling standard.

Wired Network: Commonly referred to as "the network", Wired Network is the cabling infrastructure supporting all voice, video and data transmissions, as well as the routers, switches, hubs and electronic components that facilitate technical communications. This may also be referred to as the "campus backbone network". The Wired Network begins at the point a device connects (i.e., a physical network drop or connection), continues through the campus in an intra-building mesh, and connects at a gateway to the Internet. The local access media may be fiber or copper, as appropriate for the technology.

Wireless Network: A local area network technology that uses radio frequency spectrum to connect electronic devices to the Wired Network. This may also be referred to as the wireless infrastructure, including Access Points, antennas, cabling, power and network devices used in the deployment of a Wireless Network.

6.1 Accessibility

Access to the Network Infrastructure will be provided to the Institute's staff, Interns, students, affiliates and guests, in a classification labelled "network users."

6.2 Infrastructure Policy

Implementation:
ICT: -

i. Shall be responsible for and authorized to manage and secure the Institute's networks.
ii. Will ensure physical access to those areas where network infrastructure is maintained including all circuits, firewalls, intrusion detection systems, and other enterprise network systems required to provide connectivity and to manage and/or secure the Institute's networks and data.
iii. Is authorized to establish and enforce policy and campus-wide standards for security, network and internet access, servers (application servers, DNS servers, web servers, etc.) wired or wireless technology, e-mail, web sites, network monitoring, computer technology standards, firewall policy, intrusion detection, authentication, availability of resources, network maintenance, and

for handling violations and security incidents for state owned or supported networks.

iv. Shall be responsible for identifying or developing guidelines covering cyber awareness literacy, training, and education, including ethical conduct in cyberspace.

v. Responsible for providing the secure, centralized, and standardized management of Local Area Networks (LANs) and Wide Area Networks (WANs) including policies and connectivity to enhance the implementation and management of security and thereby reduce time lost to recover from security intrusions, viruses, and "hackers."

vi. Responsible for securing the network through the effective and efficient application of resources to make satisfactory network repairs; and should detachment occur, responsible to communicate immediately with the agency to advise it of findings, cause for detachment, and commit resources to work with the agency to assist in satisfactory repair.

vii. Provide assistance to and partner with agencies in the creation of guidelines, procedures, training, and tools in order for agencies to conduct self-monitoring and self-assessment.

viii. Responsible for and authorized to perform audits on any device that attaches to the Institute's network or affects cyber security.

ix. The Institute's HICT is authorized to act in the best interest of the Institute to assign network priorities in the event of either a security incident, or the catastrophic loss of core network processing capability, and will ensure appropriate dialogue with the ICTA.

6.3 Power supply Policy

KEFRI recognize that maintenance of stable power supply is critical for protection of computing facilities. It is KEFRI's Policy therefore to use Uninterruptible Power Supply (UPS) in all computing devices within the Institute. Use of fused power extensions shall be used temporally as sourcing for appropriate UPS is underway. It is the responsibility of ICT section to inspect all UPS with the purpose of recommending for maintenance or replacement.

Power feeds to the servers shall be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.

All servers and workstations shall be fitted with UPS to condition power supply.
All switches, routers, firewalls and critical network equipment shall be fitted with UPS.
Critical servers shall be configured to implement orderly shutdown in the event of a total power failure.

Where possible generator power shall be provided to the computer suite to help protect the computer systems in the case of a mains power failure.

6.4 Wireless Networks

This policy addresses the use of IEEE 802.11 wireless data networking protocols, commonly known as "Wi-Fi" or "wireless Ethernet." These protocols are used for connecting client devices to a data network through the use of over-the-air radio signals. The primary advantages of wireless networks are mobility and flexibility. The primary disadvantages are that wireless networks are more susceptible to service disruptions, and they operate at slower speeds.

Policy Institutements

i. Access to the wireless service will be restricted to current staff, Interns, students, and guests that have been authorized.
ii. Staff, Interns and students shall be authenticated with their Domain ID where applicable. Guests will be provided a common Guest network with passwords provided by ICT staff for authentication.
iii. The wireless service shall protect authentication credentials through the use of data encryption.
iv. Users of the wireless service are responsible for obtaining a device that meets the current implementation requirements.
v. The text "KEFRI-Wireless" is reserved for defining SSID's for the KEFRI wireless service. Wireless equipment in Institute owned or leased spaces that is not part of the Institute wireless service shall not include the text "KEFRI-Wireless" in their SSID definitions.
vi. ICT reserves the right to revoke wireless service authorization for an individual KEFRI ID, Guest ID, or for any device that is disrupting the operation of the wireless service. Violation of the Institute's Network policy will result in revocation of authorization to use the wireless service.
vii. Staff, Interns, students and guests shall not install personal wireless networking equipment in Institute owned or leased spaces without written consent from ICT.

Implementation of Policy

i. Responsibility for implementing this policy rests with ICT. ICT is responsible for designing, configuring, installing, maintaining, and troubleshooting the Institute's wireless service.
ii. ICT will maintain a written description of the current wireless data networking implementation in the form of a service description. This will include device requirements for accessing the network, and information regarding procedures to obtain authorization for the deployment of user supplied wireless equipment.
iii. ICT will utilize annual budget to provide a basic level of wireless service in libraries and many common areas.
iv. ICT will provide a mechanism for procuring Guest ID's authorized to use the wireless service.
v. ICT is authorized to monitor/detect implementation of unauthorized wireless devices. ICT reserves the right to remove and/or disable wireless equipment that is in violation of this policy, and/or may disable any wired uplink data port associated with a device in violation of this policy.
vi. For more information regarding the wireless service, send email to ICT-ict@kefri.org.

6.5 Virtual Private Networks (VPN)

Policy Institutement

All users wishing to establish a real-time connection with the Institute's internal network through the Internet must employ a virtual private network (VPN) product approved by the HICT that can authenticate the user and encrypt all traffic exchanged.

Summary

The purpose of this policy is to define standards for connecting to KEFRI's network from hosts on the Internet by using a VPN to the internal network. These standards are designed to minimize potential exposure to KEFRI from damages which may result from unauthorized use of KEFRI resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image and damage to critical Information & Technology systems.

Applicability

This policy applies to all KEFRI employees, contractors, consultants, temporaries and other workers utilizing VPNs to access the KEFRI Network.

1. Remote Computer Security

Remote computers become an extension of the KEFRI network, and therefore are subject to the same rules and regulations that apply to KEFRI managed computers.

i. Software Security Patches. Remote computers must have up to date security patches for the operating system and applications that are installed.
ii. Anti-virus Software. Remote computers must have up to date and active anti-virus software (this includes personal computers) and be free from viruses.
iii. Remote Vulnerability Scanning. Remote computers using VPN technology are subject to being remotely scanned to determine that the software is current and that the system has been properly secured. Computers that do not meet the requirements will be disconnected automatically from the KEFRI network until a secure computing environment has been re-established.
iv. Non-KEFRI owned equipment. Users of computers that are not KEFRI owned equipment must configure the equipment to comply with KEFRI's VPN and Computer and Network Usage policies.
v. Approved VPN Client. Only VPN clients approved by the HICT or Network Administrators may be used.

2. Responsibilities
Users

i. It is the responsibility of users with VPN privileges to ensure that unauthorized users are not allowed to access to KEFRI internal networks.
ii. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of KEFRI's network, and as such are subject to the same rules and regulations that apply to KEFRI-owned equipment (i.e. their computers must be configured to comply with Information Security Policies).
iii. Users are responsible for communications from their computers while connected to the VPN

VPN Administrator

VPN gateways and concentrators will be setup and maintained by a Network administrator to meet minimum requirements.
i. The VPN requires the user to authenticate
ii. All communication over the VPN is encrypted
iii. All authentication attempts will be logged
iv. VPN users will be automatically disconnected from KEFRI's network after 2 hours of inactivity. The user must reauthenticate to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

3. Notification of Changes

Information & Technology will provide users with a copy of this policy (or link to it), and notify users of changes to this policy.

7. ICT security policy

RATIONALE: To provide guidelines with regard to the responsibility of every KEFRI employee who accesses Data and information in electronic formats to provide for the security of that Data. The use of Mobile Computing Devices, electronic file exchanges, and the growing use of application service providers increase the vulnerability of Institute Electronic Data and information assets. As new technologies are developed and implemented, and as new laws covering Data security emerge, issues multiply around Data management and security.

POLICY: Electronic Data are important Institute assets that must be protected by appropriate safeguards and managed with respect to Data stewardship. This policy defines the required Electronic Data management environment and classifications of Data, and assigns responsibility for ensuring Data and information privacy and security at each level of access and control.

SCOPE AND APPLICABILITY: This policy applies to all Institute personnel with access to Institute Data.

DEFINITIONS:

Confidential Data: Data that are specifically restricted from open disclosure to the public by law are classified as Confidential Data. Confidential Data require a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use. Confidential Data include, but are not limited to:

1. Student Data protected by The Kenya Communications Act (No. 2 of 1998) and as amended by the Kenya Communications (Amendment) Act, 2009, including personal identification Data such as Social Security Number, student numbers such as IDs, and other Data not classified as directory information under;

2. Medical Data, such as Electronic Protected Health Information and Data protected by the Health Insurance Portability and Accountability Act (HIPAA);

3. Research (e.g., information related to a forthcoming or pending patent application, grant applications and proposals, information related to tree subjects);

4. Information access security, such as login passwords, Personal Identification Numbers (PINS), logs with personally identifiable Data, digitized signatures, and encryption keys;

5. Primary account numbers, cardholder Data, credit card numbers,

payment card information, banking information, employer or taxpayer identification number, demand deposit account number, savings account number, financial transaction device account number, account password, stock or other security certificate or account number (such as Data protected by the Payment Card Industry Data Security Standard);

6. Personnel file, including ID Numbers;

7. Library records; and

8. Driver's license numbers, National identification card numbers, National Social Security Fund Numbers, employee identification numbers, government passport numbers, and other personal information that is protected from disclosure by state and federal identity theft laws and regulations.

Data Classifications: All Electronic Data covered by this policy are assigned one of three classifications:

1. Confidential

2. Operation Critical

3. Unrestricted

Data Custodian: Persons or departments providing operational support for an information system and having responsibility for implementing the Data Maintenance and Control Method defined by the Data Steward.

Data Maintenance and Control Method: The process defined and approved by the Data Steward to handle the following tasks:

1. Definition of access controls with assigned access, privilege enablement, and documented management approval, based on job functions and requirements.

2. Identification of valid Data sources

3. Acceptable methods for receiving Data from identified sources

4. Process for the verification of received Data

5. Rules, standards and guidelines for the entry of new Data, change of existing Data or deletion of Data

6. Rules, standards and guidelines for controlled access to Data

7. Process for Data integrity verification

8. Acceptable methods for distributing, releasing, sharing, storing or transferring Data

9. Acceptable Data locations

10. Providing for the security of Confidential Data and Operation Critical Data

11. Assuring sound methods for handling, processing, security and disaster recovery of Data

12. Assuring that data are gathered, processed, shared and stored in accordance with the Institute privacy statement posted on www.kefri.org

Data Steward: The persons responsible for Institute functions and who determine Data Maintenance and Control Methods are Data Stewards.

Electronic Data/Data: Distinct pieces of information, intentionally or unintentionally provided to the Institute in a variety of administrative, academic and business processes. This policy covers all Data stored on any electronic media, and within any computer systems defined as an Institute information technology resource under QMS policies, curse materials and intellectual property.

Hosted Solutions: Hosted Solutions include hosting by a third-party, outsourced, and application service provider software, services, or solutions. This includes cloud systems and storage. Hosted Solutions are technology solutions or systems where a third-party manages and distributes software-based services and systems, including Data manipulation or storage, appropriate to that software solution, to customers across a wide area network from a central Data center. These are usually web-based solutions where Data are sent to off-campus systems and accessed via the Internet.

Mobile Computing Devices: Information technology resources that may leave the general campus location. Samples of such devices include, but are not limited to, laptops, tablets, iPads, personal digital assistants (PDAs), cell phones, CD/DVD R/W disks, USB devices, flash drives, zip drives, etc.

Operation Critical Data: Data determined to be critical and essential to the successful operation of the Institute as a whole, and whose loss or corruption would cause a severe detrimental impact to continued operations. Data receiving this classification require a high level of protection against accidental distribution, exposure or destruction, and must be covered by high quality disaster recovery and business continuity measures. Data in this category include Data stored on Enterprise Systems such as Banner and Data passed through networked communications systems. Such Data may be released or shared under defined, specific procedures for disclosure, such as departmental guidelines, documented

procedures or policies.

Institute Provided Data Systems: Information technology resources owned by the Institute and used for the storage, maintenance and processing of Institute Data.

Unrestricted Data: Information that may be released or shared as needed. Examples are Data files for the schedule of classes or other publicly available Data such as a directory.

Usage/Data Use: Usage and Data Use are used interchangeably and are defined as gathering, viewing, storing, sharing, transferring, distributing, modifying, printing and otherwise acting to provide a Data maintenance environment.

PROCEDURES:

1. Data Stewardship

Data Stewards are expected to create, communicate and enforce Data Maintenance and Control Methods. Data Stewards are also expected to have knowledge of functions in their areas and the data and information used in support of those functions. Deputy Directors are accountable for the ultimate data management and stewardship in their respective areas of responsibility/Thematic Areas, and are the default Data Stewards for all Institute Data.

2. Data Maintenance and Control Method

Data Stewards will develop and maintain Data Maintenance and Control Methods for their assigned systems.

When authorizing and assigning access controls defined in the Data Maintenance and Control Methods involving Confidential Data, Data Stewards will restrict user privileges to the least access necessary to perform job functions based on job role and responsibility.

If the system is an Institute Provided Data System, Institute Technology Services will provide, upon request, guidance and services for the tasks identified in the Data Maintenance and Control Method.

If the system is provided by a Hosted Solution, the Data Steward must still verify that the Data Maintenance and Control Method used by the Hosted Solution provider meets current Institute technology standards. Further, ongoing provisions for meeting current Institute technology and security standards must be included in the service contract.

Review of Hosted Solutions must include Institute Technology Services and

Office of Legal Affairs prior to final solution selection and purchase.

3. Data Custodianship

Data Custodians will use data in compliance with the established Data Maintenance and Control Method. Failure to process or handle Data in compliance with the established method for a system will be considered a violation of the Institute's ICT policy and sanctions defined in that policy may apply.

4. Data Usage

In all cases, Data provided to the Institute will be used in accordance with the Privacy Statement accessed from the Institute home page www.kefri.org, and within the guidelines provided to those giving Data to the Institute (guidelines provided by the Data source).

Data will be released in accordance with Institute policies (such ICT QMS Procedures). Requests for information from external agencies (such as Freedom of Information Act requests, subpoenas, law enforcement agency requests, or any other request for Data from an external source) must be directed to the Director KEFRI.

Standards for secure file transmissions, or Data exchanges, must be evaluated by Institute ICT Division when a system other than an Institute Provided Data System is selected or when a Hosted Solution is utilized. Specific contract language may be required. The Office of Legal Affairs must be consulted regarding such language.

Unencrypted authorization and Data transmission are not acceptable.

Data Used in the pursuit of teaching, learning, research and administration must be managed to preserve integrity and trust. This is the responsibility of all who use Data.

Communications of Confidential Data via end-user messaging technologies (i.e., email, instant messaging, chat or other communication methods) is prohibited.

5. Storing data

Data cannot be stored on a system other than a Institute Provided Data System without the advance permission of the Data Steward and demonstrated legitimate need.

Data cannot be stored on a Institute-provided mobile computing device without the advance permission of the Data Steward and demonstrated

legitimate need.

Data must be stored on devices and at locations approved by Data Stewards. If information technology resources (computers, printers and other items defined in the ICT Policy) are stored at an off-campus location, the location must be approved by Property Management prior to using such resources to store Institute Data.

New technology sometimes enables the storage of Data on fax machines, copiers, cell phones, point-of-sale devices and other electronic equipment. Data Stewards are responsible for discovery of stored Data and removal of the Data prior to release of the equipment.

Data should be stored in encrypted formats whenever possible. Confidential Data must be stored in encrypted formats. Encryption strategies should be reviewed with Institute Technology Services in advance to avoid accidental Data lockouts.

When approving Mobile Computing Device Usage, Data Stewards must verify that those using Mobile Computing Devices can provide information about what Data were stored on the device (such as a copy of the last backup) in the event the device is lost or stolen.

In all cases, Data storage must comply with Institute retention policies. Data Usage in a Hosted Solution system must have specific retention standards written in the service contract. The Office of Legal Affairs must be consulted regarding such language.

Provisions for the return of all Institute Data in the event of contract termination must be included in the contract, when Data are stored on a Hosted Solution. The Office of Legal Affairs must be consulted regarding such language. Current security standards (such as controlled access, personal firewalls, antivirus, fully updated and patched operating systems, etc.) will be evaluated when a system other than a Institute Provided Data System is selected and must be covered in contract language. The Office of Legal Affairs must be consulted regarding such language.

Data stored on Mobile Computing Devices must be protected by current security standard methods (such as controlled access, firewalls, antivirus, fully updated and patched operating systems, etc.).

Institute standard procedures for the protection and safeguarding of Confidential Data and Operation Critical Data must be applied equally and without exception to Institute Provided Data Systems, Mobile Computing Devices and systems other than Institute Provided Data Systems, such as Hosted Solutions.

6. Systems and network data

Systems and network Data, generated through systems or network administration, logs or other system recording activities, cannot be used, or captured, gathered, analyzed or disseminated, without the advance permission of the Chief Information Officer, Institute Technology Services.

7. Value of data

In all cases where Data are to be processed through a Hosted Solution, the following assessment must be done:

- The value of the Data must be determined in some tangible way.
- Signature approval from the Data Steward's division vice president or appropriate party with the ability to authorize activity at the level of the value of the Data must be obtained.

8. Sanctions

Failure to follow the guidelines contained in this document will be considered inappropriate use of a Institute information technology resource and therefore a violation of Use of Institute Information Technology Resources. Sanctions will follow the steps identified in that policy.

9. Data Security Breach Review Panel

A Data Security Breach Review Panel (Panel) comprised of members of the ISMS Core team and the Head of department of the affected user will be established. If unauthorized access to Confidential Data is discovered, a member of the Panel must be contacted, who will then request the ISMS Leader to convene the Panel. This contact with the Panel must be initiated as soon as possible after the breach in order to assist the Institute in meeting its legal obligations, and may be initiated by the Data Steward, by the user of the Data, by the owner of a missing or stolen laptop or storage device, or by anyone who has become aware of unauthorized Data access.

Examples of potential data security breaches that require notification include, but are not limited to:

- Theft or loss of a laptop, desktop computer, or storage device used to store Confidential Data
- Unauthorized access to a Database system or hack of an Institute system or website.

The Panel will:

- Review the situation and assess the potential for Data exposure. It is expected that the owner of the system in question will be able to identify the Confidential Data that were stored on that system.
- Perform digital forensics necessary to assess the threat and take steps to limit the breach.
- Develop and implement a response plan to ensure the Institute's compliance with all legal and other obligations in regards to the breach.

7.1 Physical Security

System administrators and Network are responsible for establishing procedures to secure the physical environment of servers, including, at minimum: (a) locked or otherwise restricted access to server rooms, and (b) current inventory of all individuals with access to server rooms.

7.1.1 Required Physical Security

a. All KEFRI hardware shall be prominently marked, either by branding or etching.
b. All personal computers (PCs) fitted with locking cases shall be kept locked at all times.
c. Wherever possible, computer equipment shall be kept at least 1.5 metres away from external windows in high-risk situations.
d. All opening windows on external elevations in high-risk situations shall be fitted with permanent grills.
e. All external windows to rooms containing computer equipment at ground floor level or otherwise visible to the public shall be fitted with window blinds or obscure filming.
f. All doors leading to the room or area with computer equipment shall be fitted with supplementary metal grills.

7.1.2 Computer Server Rooms

a. Computer servers shall be housed in a room built and secured for the purpose.
b. The computer server rooms shall contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.
c. No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding.

d. Where possible the floor within the computer suite shall be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.
e. Access to the computer server rooms shall be restricted the authorized KEFRI staff only.
f. All non-ICT staff working within the server rooms shall be supervised at all times and the ICT section shall be notified of their presence and provided with details of all work to be carried out, at least 24 hours in advance of its commencement.

7.1.3 Access Control

a. The system Administrator in charge of a particular system shall assign system, network or server passwords for relevant access to the system after authorization from the business owner of the particular system.
b. The system administrator shall be responsible for maintaining the integrity of the system and data, and for determining end-user access rights.
c. All administration passwords of vital network equipment and of those critical Institute servers shall be recorded in confidence in case of emergencies.
d. System audit facilities shall be enabled on all systems to record all log-in attempts and failures, and to track changes made to systems.

7.2 Network and Information Security and Access Policy

Information is a valuable Institute asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies and procedures must be implemented to ensure that the integrity, confidentiality and availability of the Institute's information are not compromised.

7.3 Information Classification

All information in the Institute is classified to indicate the need to know, priorities and expected degree of protection that will be ensured while handling the information.
The Classification Categories are:
a. Confidential
b. Restricted
c. Normal

It is the responsibility of the Administration to sensitize information end-users on the Classification and handling of information in accordance with related government manuals and procedures.
Information no longer useful shall be permanently deleted from the system.
All critical information shall be securely protected; files shall be password protected and critical information shall be encrypted.
Media with confidential information shall be physically labelled.
The ICT and Administration shall be responsible for disposing media securely.
Media tapes shall be stored in lock and key at all times.

7.4 Usage Monitoring, Privacy and Surveillance policy

Users shall not assume any privacy while browsing the internet. Browsing is always monitored and some sites are restricted by use of internet monitoring software. Any user who is blocked from accessing a site which facilitates his work can, through his/her supervisor, get in touch with Head of ICT to open up the site as long as the site is safe to access and does not compromise KEFRI network.

The use of monitoring tools, such as network analyzers or similar software shall be restricted to ICT staff who are responsible for network management and security.

7.5 Passwords and Access codes Policy

It is the policy of KEFRI that: -

a. Users shall be responsible for their username and password and not reveal to other user(s). Logging on to the network with another person's details is an offence.
b. Passwords and Access codes must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
c. Passwords and Access codes must not be revealed over the phone to anyone or be inserted into email messages, or other forms of electronic communication.
d. Users must not reveal a password and Access codes on questionnaires or security forms.
e. Users must not hint at the format of a password (for example, "my family name").
f. Users must not write passwords and Access codes down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
g. Users must not use the "Remember Password" feature of applications (for example, web browsers).

h. Any user suspecting that his/her password and Access codes may have been compromised must report the incident and change all passwords.
i. Passwords must be changed when they expire i.e. no grace period, Reuse of old passwords is discouraged
j. The ICT Section will disable all passwords of exiting employees upon notification from the Head of Department.

Password Construction Requirements

a. Be a minimum length of eight (8) characters on all systems.
b. Not be a dictionary word or proper name.
c. Contain both upper and lower case characters (e.g., a-z, A-Z);
d. Have digits as well as letters;
e. Are not words in any language, slang, dialect, jargon, etc.;
f. Are not based on personal information, names of family, etc.
g. Not be the same as the User ID.
h. Expire within a maximum of 90 calendar days.
i. Not be identical to the previous ten (10) passwords.
j. Not be transmitted in the clear or plaintext outside the secure location.
k. Not be displayed when entered.
l. Ensure passwords are only reset for authorized user.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.
For example,

a. the phrase might be: "This May Be One Way To Remember"
b. the password could be: "TmB1w2R" or "Tmb1W2rr" or some other variation.

7.6 Virus protection policy

The principal concern of this Virus protection policy is effective and efficient prevention of network virus outbreaks and network security attacks involving computers associated with KEFRI. The primary focus is to ensure that KEFRI -affiliated users are aware of and take responsibility for the proper use of the KEFRI provided and supported virus protection software.
Viruses and other worm attacks can cause substantial damage to computer systems. The policy stipulates that;

a. Each employee is responsible for taking reasonable precautions to ensure that he or she does not introduce viruses into KEFRI's network

b. KEFRI provides anti-virus software to all PC's connected to the network. Any user who finds that the anti-virus software is either disabled or not functioning properly must immediately inform the ICT Section.

c. Each user is responsible for the security of any system he/she connects to the network. A system which has fallen victim to viruses/worms will be taken off the network, generally without notice, until it has been made secure

d. If any user contacts a virus from any source or receives information relating to viruses, they must immediately inform the ICT section, and follow their instructions

e. To ensure security and avoid the spread of viruses, Users accessing the Internet through devices attached to the Institute's network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer used is not connected to the Institute's network.

f. All file downloads from the Internet are automatically scanned by virus detection software.

7.7 Electronic Espionage

Any information available within ICT facilities must not be used to monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions are:

a. In the case of a specific allegation of misconduct, when the Management team can authorize accessing of such information when investigating the allegation. This may necessitate disabling the victim from accessing IT facilities pending investigation.

b. When the ICT Support team cannot avoid accessing such information while fixing a problem. The person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary.

c. Systems administrators, database administrators and auditors in their day to day work activities.

8. ICT acquisition, maintenance repair and disposal

8.1 Planning for ICT

Any ICT acquisition must have continued business justification. ICT accusation will be done by presenting a Business Case providing mechanisms to judge whether the project is (and remains) desirable, viable

and achievable as a means to support decision making in its (continued) investment.

The reasons for undertaking the project must drive decision making and the business justification will be documented in a Business Case describing the reasons for the acquisition based on estimated costs, risks and the expected benefits The Business Case will present the optimum mix of information used to judge whether the project is (and remains) desirable, viable and achievable, and therefore worthwhile investing in.

8.2 Inventory Management

An effective asset management process actively manages all hardware devices on a network, so that only authorized devices have network access, and allows for quick response to security events. Asset management consists of maintaining inventory, tracking assets, and updating records.

It is the policy of KEFRI to implement an Asset Inventory Management System application and procedures to verify assets are authorized for connectivity before adding to the system.
KEFRI management will implement a scheduled inventory verification process for sensitive property and complete plans to prevent unauthorized devices from gaining access to the network.

8.3 Maintenance Policy

It is recognized that maintenance of all ICT facilities shall be done regularly both at headquarters and in Regional Centers. It is the policy of KEFRI to support preventive maintenance on Quarterly basis using either ICT Unit or outsourced through a service contract. KEFRI will at all times guarantee to provide prerequisite resources (funds and human) for maintenance to ensure ICT facilities are sustained for provision of services. In terms of maintenance, the Head of ICT shall be expected to ensure critical systems are covered by:

a. Service contracts
b. Software system contracts with vendors
c. Detailed inventory of ICT facilities and maintenance log

This policy recognize that various levels of maintenance shall be used from time to time

a. On demand: handled on daily course of routine help desk management of issue escalation
b. Preventive maintenance scheduled
c. Local support provision for Regional Centers

It is the policy of KEFRI to provide for outsourcing through a structured framework that allows for proper vetting of vendors, management of

escalation issues to outsource (including response times) and documentation of outsourcing contracts.

8.4 Acquisition and Disposal Policy

While KEFRI recognize that all staff needs a one-on-one access to computing facilities, it also recognizes that ICT facilities have lifespan to which optimum performance can be expected.

This policy therefore stipulates that new computing facilities shall be deemed old if usage exceeds 4 years or needs replacement. Disposal shall be based on set criteria in conformity with Public Procurement and Disposal Act of 2009 and recommendations of the Disposal Committee.

ICT Section will prepare a Disposal Plan as stipulated in Public Procurement Manual for Information & Communications Technology First Edition May 2009

It is the policy of KEFRI to undertake thorough test before acceptance of all ICT devices acquired to conform to the specifications.

8.5 Asset movement and policy

9. ICT User support and training

9.1 ICT Training Policy

Vision 2030 has in mind Kenya's pool of talent is small and inadequately trained for integration into the job market. Taking cognizance of need to ensure that KEFRI retains its competitive advantage in line with its vision, there is need to ensure that ICT Staff are well trained and able to use new emerging technologies for service delivery.

To this end it is the policy of KEFRI to continuously provide training to its ICT staff on relevant ICT courses in order to ensure that they remain up to date with technology trends and serve the Institute better. Other staff will be trained on basic ICT skills at least once a year.
In order to ensure relevance and ensure that KEFRI can effectively use newly acquired ICTs, mandatory technical training shall be provided by the contractor. This training will ensure that KEFRI's ICT Staff are adequately empowered to operate, manage and use the acquired facility. KEFRI shall also endeavor to conduct continuous basic ICT for all employees.

KEFRI will build internal capacity of its staff to ensure database administrators are trained on maintaining integrated database system

9.2 User Support Policy

It is the policy of KEFRI to have a helpdesk manned by a qualified ICT staff for purpose of recording and scheduling all calls, status and recommendations received through the Helpdesk. All user requests for assistance shall be properly logged using support forms. Strategies that could be explored include:

- Provision of a common e-mail which allows all ICT personnel to receive the issues raised by staff
- Support form to be made online, which could enable users to fill the requests online
- Dedicated telephone numbers and extensions for the helpdesk.

Sensitization sessions are proposed to make users aware of escalation process as well as troubleshooting skills of simple faults not only covering hardware but also software including specialized systems.

10. Legal

10.1 Licensing policy

KEFRI ensures that all supplied computing devices are accompanied by licensed software pre-loaded into the devices while at the same time maintain genuine installation media kits. ICT Section shall maintain an inventory of all software licenses including dates for renewal and subscription where applicable. Bulk licenses shall be applied to take advantage of economies of scale and cost reduction as a result to discounts offered.

KEFRI shall where applicable negotiate licenses for all software including but not limited to Anti-virus software (corporate and single license), Microsoft Office Suite of Programs, Financial management Software, Firewall and Router license, Human Resource Management software and database software

KEFRI however recognize that alternative software shall be evaluated from time to time to ensure that the Institute use cost-effective products, including opportunities offered by open source software.
KEFRI reserves the right to inspect an employee's computer system for violations of this policy. The ICT section will conduct a regular audit of all computers (including portables) and servers, to ensure that Institute is in compliance with all software licenses. Periodic, random audits shall also be conducted as appropriate.

10.2 Downloading and Copyright Issues

You should assume that material created by others, in electronic or other forms, is protected by copyright unless such material includes an explicit statement that it is not protected or unless such material is clearly in the public domain.

Downloading a file from the Internet can bring viruses with it. Staff to scan all downloaded files with the Institute's standard virus prevention software before executing.

11. ICT Data Backup, Disaster Recovery and Preparedness Policy

The purpose of the Information Technology Disaster Recovery and Data Backup
Policy is to provide for the continuity, restoration and recovery of critical corporate and systems. KEFRI entities need to ensure critical data is backed up periodically and copies maintained at an off-site location. Entities must develop and maintain a written business continuity plan for critical assets that provides information on recurring backup procedures, and also recovery procedures from both natural and man-made disasters.

To ensure preparedness, drills shall be conducted every six (6) months to verify the ease and the extent of recovery in case of a disaster. All staff critical to ensuring business continuity of the Institute shall be trained and drilled on their roles in case natural or human based disasters occur. Precise and clear business recovery and continuity procedure manuals shall be prepared.

11.1 Data Backup Policy

The data backup policy applies to all users who use computing equipment connected to the Institute's network or who process or store critical data owned by the KEFRI. All users are responsible for arranging adequate data backup procedures for the data held on ICT systems assigned to them to ensure the recovery of data in the event of failure.

The KEFRI ICT staff is responsible for the backup of data held in central systems and related databases. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or KEFRI falls entirely to the user. All users should consult the ICT Section about local back-up procedures.

All backups must conform to the following best practice procedures:

a. The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data
b. All data, operating systems and utility files must be adequately and systematically backed up. (Ensure this includes all patches, fixes and updates)
c. Records of what is backed up and to where must be maintained
d. Records of software licensing should be backed up
e. The backup media must be precisely labelled and accurate records must be maintained of back-ups done and to which back-up set they belong.
f. Copies of the back-up media, together with the back-up record, should be stored safely in a remote location or at a sufficient distance away to escape any damage from a disaster at the main site
g. Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency
h. Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms

11.2 Disaster Recovery and Preparedness Policy

The disaster recovery policy applies to all ICT Staff who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

ICT section shall develop ICT disaster recovery plans as a critical step in the process of implementing a comprehensive disaster recovery planning program. The plan should contain detailed roles, responsibilities, teams, and procedures associated with restoring an ICT system following a disruption.

The disaster recovery plan shall document technical capabilities designed to support disaster recovery operations. The disaster recovery plan shall be tailored to the institute and its requirements.

ICT Section shall
a. Develop disaster recovery/business resumption plans.
b. Maintain and update disaster recovery/business resumption plans as need arises. Changes necessitating revision shall include changes in technology, statutory regulations and any other reasons as may be determined from time to time by the ICT Section
c. Update all users on disaster recovery/business resumption plans.
d. Test disaster recovery/business resumption plans annually and shall correct any deficiencies revealed by the test. The type and extent of testing adopted will depend on:
    i. Criticality of functions
    ii. Cost of executing the test plan

iii. Budget availability
iv. Complexity of information system and components

e. Train employees to execute the recovery plans. Training will consist of:
   i. Making employees aware of the need for a disaster recovery/business resumption plan
   ii. Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency
   iii. Training key personnel with responsibilities identified in the plan to perform the disaster recovery/business resumption procedures
   iv. Providing the opportunity for recovery teams to practice disaster recovery/business resumption skills

11.3 Backup archiving and Restore

ICT section is obliged to maintain archives of data of critical Institutional systems for a time frame that is beyond the normal backup retention period, in case of future need to refer to the data by the Institute. Archiving regime shall also be maintained in line with government policy on disposal of government documents.

For this purpose, in addition to normal backups, responsible staff shall arrange for a special backup scheduled at close of each financial year for all sensitive data on respective systems. Tapes used for this purpose shall be clearly documented and safely retained, with no intention of re-use, in a long-term storage facility.

12. Enforcement, auditing and reporting

12.1 Enforcement

The enforcement of this policy shall be the responsibility of the Accounting officer. This shall be ensured through strict adherence to the requirements of ICT security Policy

Intentional and unintentional violations of security policies and procedures must be subject to appropriate remedial advice, training or disciplinary action according to the Institute's human resources policies and procedures. Users who deliberately or repeatedly violate security policies must have their access privileges suspended until the appropriate remedial action has been determined.

Violations of this policy, depending on severity and nature, may result in reprimand, loss of ICT privileges, or termination of employment.

12.2 Audit

ICT section shall conduct audits and surveys once yearly to assess the levels of implementation of ICT Security Policy.
For the purpose of performing an audit, any access needed shall be provided to members of the audit team when requested. This access shall include:

- User level and/or system level access to any computing or communications device.
- Access to information (such as electronic or hardcopy) that may be produced, transmitted or stored in the Institute's infrastructure.
- Admission to interactively monitor and log traffic in the Institute's ICT networks.

12.3 Reporting

All employees and third party users of the Institute's infrastructure will be aware or made aware of their responsibility to report any information security incidents and/or weaknesses in systems or services.

All users shall report any breach of policy and weaknesses through the head of departments to the head of ICT section.

13. Revision

This policy shall be revised on an annually basis. Changes necessitating revision shall include changes in technology, statutory regulations and any other reasons as may be determined from time to time by the Head of ICT.

14. Reference

a. ISO 27001:2013
b. Government ICT standards
c. Records management procedures manual for the public service, May 2010
d. Kenya National Archives and Documentation Services Act (1965)
e. Public Procurement Manual for Information & Communications Technology First Edition May 2009
f. Public Procurement and Disposal Act of 2009

15. Approval

This is to confirm that this document, the ICT Policy for Kenya Forestry Research Institute (KEFRI) has been approved by the management for implementation:

Signed :

Name : Dr. Ben Chikamai PhD

Designation: Director, KEFRI