

KENYA NATIONAL LIBRARY SERVICE

ICT POLICY

VER. 1

Definitions and abbreviations

Information and Communication Technology	- ICT
Gross Domestic Product	- GDP
Kenya National Library Services	- KNLS
Closed Circuit Television	- CCTV
Radio Frequency Identification	- RFID
Library Management System	- LMS

Table of Contents

Definitions and abbreviations	ii
Preamble.....	v
1. Introduction	1
1.1 What is ICT?	1
1.2 Vision of ICT Policy	1
1.3 MISSION of ICT Policy.....	1
1.4 Objectives of ICT Policy	1
1.5 Key stakeholders	1
2. Key Policy Areas.....	3
2.1 Training.....	3
2.2 Accessibility	3
2.3 Innovation in Technology	4
2.4 Digital Content/Repositories	4
2.5 Power supply	5
2.6 Maintenance.....	5
2.7 E-mail use	6
2.8 Website	6
2.9 Internet use	6
2.10 System Integration	6
2.11 New Systems Changeover	7
2.12 Acceptable use.....	7
2.13 Infrastructure.....	9

2.14	Disposal and Acquisition.....	10
2.15	User support	10
2.16	Partnership	10
2.17	Security.....	11
2.18	Library Management System.....	12
2.19	Finance System	13
2.20	Human Resource System.....	13
2.21	Licensing policy	14

Preamble

Kenya National Library service (KNLS) is a statutory body of the Government of Kenya established by an Act of Parliament, Cap 225 of the Laws of Kenya in April 1965 with a mandate to develop, promote, establish and equip libraries in Kenya.

The fourth strategic objective of KNLS strategic Plan 2009 - 2013 clearly states that KNLS will integrate ICT in library operations and service delivery in order to meet the goals of the Government of Kenya's Vision 2030 which covers Kenya's development blueprint for the period 2008 to 2030. It aims to transform Kenya into a newly industrialize, "middle-income country providing high quality life to all its citizens by the year 2030". The Vision is anchored on three "pillars": the economic, the social and the political. Vision 2030 is the successor for another successful plan known as Economic Recovery Strategy for Wealth and Employment Creation (ERS) which has enabled the country's economy revert back to the path of rapid growth since 2002, when GDP grew from a low of 0.6% and rising gradually to 6.1% in 2006 and 6.3% in the first quarter of 2007.

KNLS operates more directly under the Social Pillar. Eight key social sectors are targeted under the social pillar. These are education and training; health; water and sanitation; environment; housing and urbanization; as well as gender, youth and vulnerable groups. Each of the sectors will benefit from the contribution of KNLS as it pursues the objectives in the strategic plan within the context of its mandate.

Simply put, transformation of Kenya will not occur without proper management of information within a sound framework that will ensure KNLS is well coordinated and harnessed.

This ICT Policy will go a long in ensuring that KNLS operates a well structured ICT system.

1. Introduction

1.1 What is ICT?

Information and Communication Technology (ICT) is defined by KNLS as a diverse set of technologies used internally and externally to gather, communicate, create, disseminate, store and manage information. ICT include but not limited to Computers, Internet, printers, scanners, radio, television, telephone, talking books, software, cellular phones, networks and network devices.

1.2 Vision of ICT Policy

- To use ICT as a dynamic tool of choice in provision of library and information services

1.3 MISSION of ICT Policy

- To enhance access, accurate and relevant library and information services through integration of ICTs.
- To enhance availability of information resources and preservation of national imprint through integration of ICTs in library service.

1.4 Objectives of ICT Policy

It is expected that this policy will help KNLS re-engineer its processes with a view of efficient and effective delivery of library and information services. Specific objectives of the policy include:

- To define the scope of what is ICT in KNLS
- To open up KNLS libraries to new users
- To open up new services to existing users
- To serve as a guideline to KNLS staff and public on what is good or not good ICT practice in terms of usage of Information Systems facilities
- To serve as a guideline for ICT resource allocation
- To serve as a guideline for staff on ICT practice and procedures
- To serve as a guideline for modernizing KNLS services
- To enhance customer satisfaction
- To enhance service integrity and transparency
- To enhance communication speed
- To promote KNLS service through the web.

1.5 Key stakeholders

- Ministry of State for National Heritage and Culture
- Kenya ICT Board

- Kenya Education Network (KENET)
- Ministry of Information and Communication
- Development partners
- Users
- Telkom Kenya
- Safaricom
- Kenya Data Network
- Computer Aid International
- Computer for All Africa

2. Key Policy Areas

2.1 Training

Taking cognizance of need to ensure that KNLS retains its competitive advantage in line with KNLS vision, there is need to ensure that employees are well trained and able to use new emerging technologies for service delivery.

To this end ***it is the policy of KNLS to continuously provide training to its members of staff on relevant ICTs in order to ensure that customers get the best service when they need it.***

In order to ensure relevance and ensure that KNLS can effectively use newly acquired ICTs, ***mandatory technical training shall be provided by the contractor. This training will ensure that KNLS is adequately able to operate, manage and use the acquired facility.***

At the same time, departments and branches will be involved in assessing training needs for users. This will then feed into recommendations to Staff Training Committee. However, recommendations to us local trainers will be given priority as a time and cost cutting measure.

Departments or functional area within KNLS shall be responsible for ensuring adequate system administration training and capacity exist within the department. This means that functional or departmental heads will be responsible for ensuring that system administrator in their area is adequately trained and competent to manage the system. ***It is also the policy of KNLS that system administrator(s) will provide basic training for new and old users whenever necessary. It is also the policy of KNLS that technical training of ICT staff and system administrators shall be given priority.***

KNLS ***shall endeavour to conduct continuous basic ICT for all employees***; this shall require significant investment and resources.

2.2 Accessibility

It is the policy of KNLS to make the library reading materials accessible to all customers. To this end, KNLS shall use ICTs to enhance access to all categories of users without discrimination. Deliberate effort shall be made to ensure that children, the old and visually impaired customers get access to ICTs for reading and learning purposes.

KNLS shall ensure that all branches have staff trained to support Visually Impaired Persons using the library for reading purposes. ***It is the policy of KNLS that all libraries shall be equipped with screen reader and magnifier software for the visually impaired.*** KNLS shall also acquire e-books for popular academic books, journals and literature to open up the world of research and learning to the visually impaired.

Most KNLS libraries have sections dedicated to children. So as to make the children part of ICT development; within this policy framework, ***KNLS shall provide at least one computer for all branches for exclusive use by children.***

To make ICTs available and accessible in all branches of KNLS, deliberate effort shall be made to ensure that all branches have power supply and Internet. ***It is therefore the policy of KNLS to use alternative source of energy and Internet access in all remote stations.*** These include use of solar and wind power as well as other innovative methods.

2.3 Innovation in Technology

Innovation in organizations can be stifled by lack of adequate framework under which to operate. This means that innovative and hard working staffs are forced to look for alternative organizations ready to accept and incubate the innovations.

KNLS recognizes the need to provide an enabling framework for its staff to research and innovate. To this end KNLS encourages innovation among its staff. To ensure that this is done in an orderly manner, staff seeking to innovate shall seek approval from Director of KNLS prior to starting such projects. The request must include proposal and associated documentation. KNLS encourages innovations that are self sustaining with good proof of financial backing from funders.

Where innovations are being done jointly with external entities, proof of partnership credibility and commitment (financial and in kind) shall be provided to Director prior to approval. Where innovation involves Intellectual Property, necessary legal steps must be put in place to safe guard interest of KNLS.

It is therefore the policy of KNLS to encourage innovations that are in line with KNLS mandate. KNLS shall endeavour to compensate employees that shall innovate and improve KNLS standing in line with KNLS corporate vision and mission.

2.4 Digital Content/Repositories

KNLS recognize that most of the information resources shall be in digital form as web resources/ electronic journals, accessible within KNLS Centres or without. ***It is therefore the policy of KNLS to continuously modernize all its Centres 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 KNLS.

This policy recognizes that KNLS 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 KNLS will not be held responsible for any use or otherwise by its clients other than the purpose intended (education and information repository).*** It is expected that KNLS will continue with use of OPAC in the management of library resources, while providing link to subscribed local and international repositories.

2.5 Power supply

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

KNLS will have a standby generator which should be primed to ensure no damage to computing devices in case of power failure. KNLS shall continue with sourcing for alternative power sources especially for branches and remote areas which has KNLS centres.

2.6 Maintenance

It is recognized that maintenance of all ICT facilities shall be done regularly both at headquarters and in remote sites. ***It is the policy of KNLS to support preventive maintenance a minimum of twice per year using either ICT Department or outsourced through a service contract.*** KNLS will at all times guarantee to provide prerequisite resources (funds and human) for maintenance to ensure ICT facilities are sustained for provision of library and information services. KNLS will provide the same maintenance to branch and remote offices with continuous evaluation of outsourcing to vetted vendors and support from partners.

In terms of maintenance, ICT Department shall be expected to ensure critical systems are covered by:

- Service contracts
- Software system contracts with vendors
- Detailed inventory of ICT facilities and maintenance log

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

- On demand: handled on daily course of routine help desk management of issue escalation
- Preventive maintenance scheduled

- Local support provision for branches

It is the policy of KNLS 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.

2.7 E-mail use

KNLS e-mails are provided for to all staff on prefix @knls.ac.ke. The format shall follow the convention shown below unless stated otherwise.

{firstname.lastname@knls.ac.ke}

It is the policy of KNLS to have e-mail recognized as official means of communication. E-Mail archiving regime shall also be maintained in line with government policy on disposal of government documents.

2.8 Website

It is the policy of KNLS to update the website frequently on current issues happening within the organization with respective departments expected to forward information to the Communication and Public relations Office for vetting before ICT Department uploading the information to the website. KNLS will work out a framework that allows respective departments to manage own content on the website.

It is the policy of KNLS to use website as a key marketing tool for its services. Hosting and website development shall be outsourced so as to ensure that KNLS gets best designed and stable website.

2.9 Internet use

Access to Internet shall be provided to all staff for official use on research and collaboration. KNLS however reserve the right on the content accessed and the users allowed to access Internet. ***For access to blocked sites, necessary permissions can be sought in writing to Head of Department concerned for consideration.***

ICT Department shall be expected to facilitate installation of tools for bandwidth monitoring, downloads and report generation for decision making on Internet usage.

2.10 System Integration

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

2.11 New Systems Changeover

With increasing automation and modernization of KNLS processes for efficient service delivery, systems will be integrated and new systems developed. This necessitates the need for this changeover policy to allow the organization, for smooth adoption of the systems with minimal disruption of library and information services.

This policy proposes use of changeover strategies such as parallel runs, integration testing, and acceptance testing amongst others. ***It is the policy of KNLS therefore that before any major system changeover, a changeover strategy must be in place and agreed with end users and stakeholders before changeover.*** Parallel runs and testing shall run for a period agreed on with all concerned.

2.12 Acceptable use

While KNLS provides ICT facilities for use by staff for research and access for library or information services, the right to access and use such facilities shall be controlled by guidelines developed and shared with all users. KNLS shall avail ICT facilities on a timed schedule for equitable access.

External devices brought to the KNLS shall be prohibited unless adequate measures are taken in consultation with ICT Department to ensure safety of library and information services.

The following guidelines shall apply:

- a) Kenya National Library Services (KNLS) shall provide access to computers and the Internet to support research and educational needs of all users.
- b) KNLS shall offer cyber café services in all major branches at reduced costs.
- c) So as to protect KNLS integrity and guard against liability due to improper use of Internet, children (defined as below 17 years) shall need parental permission from a parent or guardian to access the Internet from KNLS cybercafé.
- d) Personal laptops brought by users shall not be allowed on KNLS network without prior written consent from branch Librarian or Head of Department.
- e) Material that are offensive, pornographic, hate material or promoting tribalism, sexism and so on shall not be accessed or distributed through KNLS network.
- f) Users shall be made aware of terms and conditions set out in this Acceptable Use Policy. User who do not agree with this policy shall not be allowed to use ICT facility.

g) Children Acceptable Use

The following information apply for children under the age of 17 years with reference to use of ICT facility. This information shall made available on a notice board in all branches:

- You will need to have permission from your parents or guardian to use the Internet
- KNLS will provide permission form which must be signed and returned back to the library before you're allowed to use the Internet
- Depending on number of people waiting to use computers, the Librarian will allow you to use the computer for a period of 1 hour.
- KNLS Internet accessed is filtered meaning some websites are not accessible.
- Instant Messaging or inappropriate social networking sites are not allowed.
- Kindly ask for help to save your work on a USB stick or other form of external drive. This must be checked for viruses before use.
- Foreign software must not be installed onto the library computers.
- Do not use software that creates noise or distracts other users.

h) Unacceptable Use

- KNLS prohibit use the ICT facilities in any way which may result in a breach of the:
 - i. Kenya Copyright Act
 - ii. Protection of Children Act;
 - iii. Sexual Offences Act;
 - iv. Public Order Act;
 - v. Any other Act prohibited by Parliament.

i) Downloading and Copyright Issues

- You can download material from the Internet in accordance with copyright restrictions.
- KNLS does not allow these materials to be stored on its computers; therefore arrangements must be made with KNLS staff for storage on USB memory stick.

- Copyright restrictions relating to the scanning of books, journals and magazines apply to all materials in KNLS library. A member of KNLS library staff shall be in position to help in case of doubt. The following rules apply:
 - i. Photocopying or scanning of complete works is prohibited
 - ii. Permitted extracts can be photocopied or scanned for private use.
 - iii. Only a single copy of a given page can be made
 - iv. No more than one article per journal/magazine issue may be copied

2.13 Infrastructure

This policy stipulates that KNLS shall put in place measures that ensure privacy, safety of information and data and equitable access to ICT resources. Appropriate configuration shall be put in place to ensure Computing devices do not expose user's identity and information to unauthorized persons. Whereas ICT Personnel with administrative rights can access any computing facilities, this policy will ensure such privileges are under control.

This policy empowers KNLS to apply filtering tools in order to block unsolicited content which could harm staff in using computing facilities. Blocking shall employ strategies not limited to blocking of file downloads exceeding set size threshold, monitoring general e-mail attachments and downloads, and employing content monitoring tools.

KNLS policy also is to expand the use of networked computing facilities to enhance data and information sharing and common use of scarce resources such as printers and scanners. Local Area Networks (LAN) shall be expanded in all branches, use of virtual private networks (VPNs) to ensure remote locations (branches) access services at the headquarters.

To ensure infrastructure components deliver intended purpose, ***it is the policy of KNLS that specifications used by procurement department shall be updated from time to time but at a maximum every six (6) months by ICT Department to ensure currency and value for money on acquisition.*** This policy therefore requires that vetting of pre-qualified vendors shall be done collaboratively by ICT Department, Procurement and Administration to ensure trustworthy, quality of procurement process and integrity in the acquisition of ICT facilities.

KNLS shall take into consideration trends in technology and use the LMS in conjunction with emerging technologies such as Smartcard and RFID (Radio Frequency Identification tags) in order to make best use of ICT in delivery of services.

KNLS will put in place Closed Circuit TVs (CCTV) to help monitor book shelves against books vandalism. In this case, IP based CCTV with in built intelligence shall be used to predict and proactively monitor suspect cases.

2.14 Disposal and Acquisition

While KNLS 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 6 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 KNLS Disposal Committee.

KNLS recognize that donated ICT facilities pose a challenge of disposal as some are unserviceable and costly to repair. ***This policy therefore requires that all ICT donations accepted shall be based on prescribed guidelines of KNLS with minimum specification developed by ICT Department used at all times. Minimum specifications shall be developed by ICT department every six (6) months and circulated to relevant departments.***

This policy also requires the ICT Department, Finance and Procurement Departments to maintain an up to date inventory showing the age limits of each computing facility to guide acquisition process for replacement.

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

2.15 User support

It is the policy of KNLS to have a helpdesk manned by a qualified ICT expert 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 ict@knls.ac.ke
- Support form to be made online, which could enable users to fill the requests online
- Dedicated telephone numbers and extensions for the helpdesk.
- Emergency numbers to be used during non-working hours.

KNLS also proposes various sensitization sessions 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 developed.

2.16 Partnership

For KNLS to fully empower all staff and its branches, it will take involvement of various partners offering training, facilitating acquisition of ICT facilities and resources (human and

funds). As recognized from past, some of the partners have brought to KNLS equipment of suspicious quality, some non-functional.

It is therefore KNLS policy to guard against any dumping from any partner by ensuring all assistance is in conformity with KNLS acceptable specifications and standards and right to choose what is taken from any consignment.

Whereas partnership is not limited to donations, KNLS commits to take advantage of partnerships that could empower its staff and branches. Notably, KNLS recognize that branches which are resource centres could also be used as part of digital villages or learning centres, and hence get support on equipment and connectivity from Ministry of Information and Communication and affiliate partners.

2.17 Security

Information is a critical asset. KNLS generates, stores and provides access to its clients. This resource attracts varied threats ranging from hacking, unauthorized access, vandalism and alterations. It is therefore the policy of KNLS to ensure information is safeguarded while in storage, transit or being accessed or used by any of its staff and clients.

KNLS shall use filtered Internet service in order to block access to inappropriate websites. In order to ensure that research and education is not curtailed by filtering, KNLS shall release blocked websites once verified as not harmful.

Appropriate strategies shall be applied to ensure security of information:

- Password use to access computing devices including sensitive documents. KNLS shall develop appropriate guidelines to ensure the Password use is understood and that staff changes the passwords periodically to enhance security.
- KNLS staff 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 punishable offence..
- Passwords shall expire every 6 months if not changed within that period.
- The length of the password shall not be less than six (6) characters.
- Measures shall be put in place to counter hacking activities which may lead to loss of KNLS information and disruption of services. Monitoring tools shall be acquired and installed for use by ICT Department to ensure such threats are minimized.
- Firewall system shall be improved to ensure high availability of Internet services and web services offered to KNLS clients. Current configuration shall be enhanced to provide redundancy and diverse tools for monitoring performance and threats.

- Backup shall be facilitated to ensure KNLS is prepared for recovery from any form of disaster on its information and communication infrastructure. Staff shall also be trained on backup strategies so as to safeguard any loss of data and information resources within KNLS computing devices.
- All computers shall have running anti-virus software but KNLS cannot guarantee total protection from viruses when using the library computers. E-mails sent to and from KNLS mailboxes will be scanned for viruses.

2.18 Library Management System

KNLS uses a Library Management System (LMS) for management of its library services and resources. The system currently serves the headquarters with plans to have the system features extended to branches once prerequisite infrastructure is in place.

Library Management System is the ICT system driving KNLS core business of library service provision. The range of services offered by LMS through shall include: acquisition of stock, maintenance of the library catalogue, stock movement, membership records, charges, customer loans and requests for items, and management information reports.

In the era of the Internet, the LMS shall provide web based OPAC facility to enable KNLS deliver Online Access to customer services.

It is the policy of KNLS that the LMS must have facility to host e-books, PDF versions of daily newspapers, government documents such as sessional papers, policy documents and journals that KNLS archives for reference by users regardless of age or disability.

It is the policy of KNLS to integrate digital repositories such as DSpace with LMS to ensure a seamless single point of access for users. This should enable archiving of important national resources such as traditional folklore and historical speeches and videos.

Using technologies such as **Virtualizations**, access to different National Museum and National Archives shall be achieved by KNLS.

In order to ensure that LMS operates within the mandate and in line with library operational rules and regulations, a System Administrator shall be appointed to manage LMS on behalf of the functional department.

It is the policy of KNLS that the Library management system shall have a designated Systems Administrator. The main qualifications for the Systems Administrator shall be sound knowledge of Library and Information Science with good training on use of the Library Management System.

This training shall be provided by the supplier. The systems Administrator shall be responsible for training and inducting new users to the system as well as ensuring that correct access levels for all users. The system Administrator will be responsible to the

Deputy Director in charge of Library operations on integrity and proper operation of the Library Management System. The System Administrator shall also work closely with ICT Department.

2.19 Finance System

KNLS has Finance Management Software (FMS) to manage its finances. KNLS shall explore all means of integrating all related systems with FMS to enable database sharing between systems. It is recognized that the Financial System has varied user rights which allow access to various components of the financial module, given guarantee for integrity of data and information access.

ICT Department shall be strengthened to support the system by providing backup services, supervision of the service level agreements with the supplier and skills to manage system maintenance.

It is the policy of KNLS that the financial system shall have a designated Systems Administrator. The main qualifications for the Systems Administrator shall be sound knowledge of Accounting and finance with good training on use of the Financial Management System.

This training shall be provided by the supplier. The systems Administrator shall be responsible for training and inducting new users to the system as well as ensuring that correct access levels for all users. The system Administrator will be responsible to the Deputy Director in charge of Finance on integrity and proper operation of the Financial Management System. The System Administrator shall also work closely with ICT Department.

2.20 Human Resource System

Like all other systems, KNLS will pursue an integration policy to ensure all systems use shared data structures as possible, hence achieving shared data and minimal duplication of information and effort. Human resource system has all functionality to serve the staff of KNLS, with modules covering payroll, staff details, allowance management, progression amongst others.

The Policy is to have the system provide for integrity checks, data consistency and allowance for expansion, integration with other systems and decentralization.

The Human Resource Management System shall have a designated Systems Administrator. ***It is the policy of KNLS that the Human resource management system shall have a designated Systems Administrator. The main qualifications for the Systems Administrator shall be sound knowledge of Human resource Management with good training on use of the human Resource Management System.***

This training shall be provided by the supplier. The systems Administrator shall be responsible for training and inducting new users to the system as well as ensuring that correct access levels for all users. The system Administrator will be responsible to the Deputy Director in charge of human resource or administration on integrity and proper operation of the Human Management System. The System Administrator shall also work closely with ICT Department.

2.21 Licensing policy

KNLS ensures that all supplied computing devices are accompanied by licensed software pre-loaded into the devices while at the same time maintain Compact Discs (CDs) or DVDs. ICT Department 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.

KNLS shall negotiate licenses for all software including:

- Anti-virus software (corporate and single license)
- Microsoft Office Suite of Programs
- Financial management Software
- Library System
- Cyber roam router license
- Human resource management software

KNLS however recognize that alternative software shall be evaluated from time to time to ensure organization use cost-effective products, including opportunities offered by open source software.

3. Disaster Recovery and Preparedness

Taking into consideration the current developments within the central government with regards to new infrastructure such as Government Common Core Network (GCCN) and data centres being established through e-Government Directorate; ***it is the policy of KNLS to maximize on these existing infrastructures so as to cut down on time and cost.***

KNLS will therefore leverage on these existing network for both its operational and back up network. Within this framework, KNLS shall use of government National Data Centre as its preferred first line of back up and disaster preparedness.

It is the policy of KNLS to use off-site Data Centres for back up of critical corporate data.

To ensure preparedness of KNLS drills shall be conducted every six (6) months to verify preparedness. All officers critical to ensuring business continuity of KNLS 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 under leadership of Director KNLS.