ICT Policy for Jinja Regional Referral Hospital,
Ministry of Health, Uganda.

29th April 2019

National Information Technology Authority (NITA-Uganda)

Submission by John Mark SEMAKULA
+256774486393 / +256704486393, marksemakula1@gmail.com, Skype: @marc17051, Twitter: @marc1705

Table of Contents

General Scope 5
ICT Governance Policy 5
Introduction 5
Policy Scope 6
Policy Statements 6
The Committee on ICT 6
The heads of departments and Units, Teaching staff, Administration and Hospital Management committees 7
Staff and Student Community 7
Hospital ICT Infrastructure, Networks and Service Management 7
Introduction 7
Policy Scope 8
Objectives 8
Digital networks, Servers and overall components 8
Definition 8
Hospital Local Area Network 9
Definition 9
Structure of Hospital LAN 9
JRRH Wireless Access 10
Definition 10
Structure of JRRH Wireless Access 10
Access Control, Data Protection, Cyber Security and Remote Access Policy. 11
Introduction 11
Policy Statement 11
Password Policy 11
Closed-Circuit Television (CCTV) System and Unified Intercom Telephony Services Policy 11
Server rooms, Network Equipment and general ICT software, hardware and Data Policy. 12
Policy Approach 12
Suspension and/or Termination of Access 12
Remote Access 13

Policy Scope 14
Disaster Recovery & Business Continuity Plan. 14
Definition 14
Social Media (Social Networking), Proprietary, Open Source and Privately owned / BYOD (Bring Your Own Device) ICTs 15
Introduction 15
Policy Objective 15
Policy Scope 15
Policy Statements 15
Bring your Own Device / Personal ICTs 16
Statement of Liability 17
Policy Approach 17
ICT Services Support or maintenance, development, licensing and Procurement 17
Introduction 17
Policy Objective 17
Policy Scope 18
Policy Statement 18
Roles 18
Technology Service Support 18
Responsibilities of ICT Tech Services Support personnel 19
Policy Approach 19
ICT Skills Capacity Building, Gender and E-Learning Policy 19
Introduction 19
Policy Objectives 20
Policy Scope 20
Policy Statements 20
ICT Capacity Building Assessment 20
Special Needs ICT Usage Policy 21
Introduction 21
Policy Objective 21
Policy Scope 21

Policy Statements 21
Policy Approach 22

General Scope

The ICT policy applies to all Jinja Regional Referral Hospital Departments, Clinics, all Units, all users, stakeholders, service providers, partners and users of ICTs including Developers & resource administrators; and covers -

i. ICT Governance

ii. Access Control, Cyber Security, Confidentiality and Data Protection

iii. Hospital ICT Networks and Service Management

iv. ICT Skills Capacity Building

v. ICT Services Support, development, licensing and Procurement

vi. Social Media, Proprietary, Open Source and Privately-owned ICTs

vii. Disaster Recovery and Business Continuity Plan

viii. Special Needs ICT Usage

ICT Governance Policy

Introduction

Jinja Regional Referral Hospital is located in Eastern Uganda; the hospital was opened in the early 1920s and is currently one of the 13 Regional Referral Hospitals in Uganda under the Ministry of Health.

Effective ICT Governance provides a conducive environment for the alignment of all ICT investments in a rationalized manner that is aligned towards enabling an organization meet its goals and objectives. This also contributes to the attainment of value for money, management of risks and effective ICT utilization.

- The Hospital shall provide for the centralized effective Governance of all ICT related matters within the Hospital in a rationalized and harmonized manner.

Policy Scope

This policy applies to all ICT related matters within the Hospital.

Policy Statements

The Committee on ICT.

There shall be a committee on ICT. The Committee on ICT will have its representation as determined by the Hospital management. The Committee shall:

I. Advise and monitor the implementation of the ICT Strategy, ICT Services and Policy;

II. Advocate for provision of resources within the Hospital Budgeting process for implementation of the ICT Strategy through:

    a. Agreeing on an amount for budgetary allocation to ICT.
    b. Seeking grants for ICT support in the hospital.

III. Advocate supervise sustainable ICT solutions that are aligned to the Hospital's strategic goals;

IV. Advise on and access ICT threats in the hospital.

V. Undertake advocacy for the adoption and utilization of ICT within the Hospital.

The heads of departments and Units, Teaching staff, Administration and Hospital Management committees.

The Heads of Departments shall in consultation with committee:

a. Integrate ICTs into their activities;
b. Implement and ensure compliance to the ICT Policy Framework; and
c. Act as active participants during the periodic stakeholder consultations towards supporting and facilitating the effective implementation of the ICT Policy and Strategy.

Staff and Student Community

The Staff and Student Community shall ensure strict compliance to the ICT Policies.

Hospital ICT Infrastructure, Networks and Service Management

Introduction

The Hospital ICT Infrastructure services shall be broken down into the following areas:

I. Digital networks and Servers
II. Hospital Local Area Networks (LANs)
III. JRRH Wireless Access

IV. Remote Access
V. User Privileges and Access Control for Computing infrastructure and ICT services

Policy Scope

Objectives

The objective of this Policy is to guide the development, rollout, maintenance and usage of the Hospital ICT Infrastructure and services to ensure resiliency, stability and higher uptime rates. This is all working towards ensuring that usage is aligned to the goals of the Hospital as laid out in the Hospital Strategic Plan.

The Hospital shall provide a resilient, secured and stable fast data communications network as an enabler to processing, storage, dissemination and accessing of information or ICT enabled services as relates to the various needs of the medical, support, administration and research users.

The Hospital shall establish and maintain a Data Center to act as a central

repository for all Hospital databases;

Introduction of new technology within the network management or provision shall undergo professional testing including User Acceptance Tests (UATs) to ensure compliance with oversight of the committee on ICT and existing standards / performance requirements;

Digital networks, Servers and overall components

Definition

These in this case refer to networks incorporating both switching and transmission of electronic resources that are not controlled or a product of the hospital.

a) The management of the entire digital network infrastructure shall be vested with the committee on ICT;

b) The committee on ICT shall periodically define the methodology for access to external data resources;

c) The Hospital shall establish central monitoring and control the Hospital-wide digital network

d) All core network components shall be designed to support redundancy for continued service provision;

Hospital Local Area Network

Definition

The computer network within each Hospital building shall form a Hospital Local Area Network (LAN) and will have a designated technical administrator under the supervision of the Unit responsible for ICT.

Structure of Hospital LAN

a) The Hospital shall provide secured and resilient Hospital LANs

b) All Hospital LANs will ensure compliance with approved Hospital ICT structured cabling standards and network configurations

c) All Hospital LAN extensions or modifications shall require approval from the Unit responsible for ICT

d) The Network health monitoring and technical support shall be the responsibility of the Unit responsible for ICT.

JRRH Wireless Access

Definition

Wireless Access refers to the provision of connectivity to the internet using wireless technology through authorized Access Points.

Structure of JRRH Wireless Access

a) The Hospital will support the provision of reliable and secured near-ubiquitous Wireless Access Points across the Hospital Resources;

b) Only approved Wireless Access Points shall be allowed to transmit wireless signals;

c) The configuration of such Wireless Access Points shall comply with approved network and security configurations to achieve consistency and performance standards;

d) The Wireless Access health monitoring and technical support shall be the responsibility of the unit responsible for ICT.

Access Control, Data Protection, Cyber Security and Remote Access Policy.

Introduction

Cyber security in this context refers to the protection of Hospital digital infrastructure and information assets against any compromise or attack that may affect its confidentiality, integrity and/ or availability.

The objective of the policy is to ensure safety of all ICT infrastructure of the hospital and information there-in against cyber threats and physical malicious attacks from time to time.

Policy Statement

Password Policy

All users shall ensure the privacy of their passwords

The committee on ICT shall advise on the password strength and lifecycle specification for all user categories from time to time

All default system or hardware passwords shall be changed by technical person as defined by management.

The committee on ICT shall implement and maintain centralized authentication, authorization, and accounting service mechanism for all network core equipment to all ICT resources

Closed-Circuit Television (CCTV) System and Unified Intercom Telephony Services Policy

Definition

A TV system in which signals are not publically distributed but are monitored primarily for surveillance and security purposes.

There shall be Implementation of CCTV for access monitoring of all Hospital buildings and entry points

Server rooms, Network Equipment and general ICT software, hardware and Data Policy.

a) The committee on ICT shall maintain an updated ICT asset register

b) Ensure the controlled and audited usage of ICT administrative privileges

c) Access to Hospital Server rooms and other network equipment and installations shall be secured and only allowed to authorized personnel;

d) All network equipment and/or installation shall be labelled according to the Hospital approved ICT nomenclature specification;

e) All Hospital units shall maintain a service schedule for all network equipment;

f) All installations of network equipment by academic staff for educational purposes shall be authorized by the Unit responsible for ICT;

g) The committee on ICT shall define and manage all Service Level Agreements with third party service providers for provision of maintenance and any other ICT related service, Authorize and supervise contractors or any stakeholder with third party access to the hospital ICT infrastructure.

Policy Approach

Suspension and/or Termination of Access

The following constitute reason for user access termination to Hospital computing resources:

a) Lapse or end of staff, volunteer or student contractual tenure

b) Request from Hospital Management, Heads of Department and/ or Hospital Human Resource Department.

c) Any user action that contravenes the Computer Misuse Act (2011) or the Anti-Pornography Act (2014).

d) Unauthorized Sharing of individual access passwords and privilege rights.

e) Violations of the rights of any person or company protected by Uganda's copyright, trade mark, patent, or other intellectual property (IP) law and the Hospital's Intellectual Property Policy, other relevant policies, or the Hospital's code of conduct.

f) Using hospital resources for personal commercial gain, sending spam, blackmail and solicitation.

Remote Access

Definition

The Hospital will support the provision of remote access for approved Hospital resources. This supports the provision of access to network resources to authorized users across public internet infrastructure with consideration for information security.

Structure of Remote Access

a) The committee on ICT shall define and implement the remote access methodology, technology, standards and monitoring as the requirements to ensure privacy and security

b) Remote Access shall only be provided to:

Users approved by management or the committee on ICT as per the business need requirement

c) All approved users for the remote access functionality shall consent to the Cyber Security Policy requirements for remote connections; and

Policy Scope

This Policy applies to all Hospital owned ICT infrastructure, digital information and services.

Disaster Recovery & Business Continuity Plan.

Definition

These are a set of policies, tools and procedure to enable recovery or continuation of vital ICT infrastructure after natural or man-made disaster.

The hospital shall maintain an updated and tested Business Continuity and Disaster Recovery Plan for all critical Hospital digital infrastructure and information assets by;

i. Implementing periodic systems and infrastructure audits.
ii. Maintaining and updating a documented secure configurations manual for all hardware and software

iii. Monitoring real time analysis of all ICT network device event security logs with a centralized mechanism

User electronic information may be accessed for the purposes of ensuring continuity in hospital operations. This need can arise for instance if an employee who typically has access to the files in question is unavailable due to illness or vacation

Social Media (Social Networking), Proprietary, Open Source and Privately owned / BYOD (Bring Your Own Device) ICTs

Introduction

Social media is referred to as any internet-based service that provides electronic social interaction amongst its users and communities.

Policy Objective

To guide the appropriate usage of social media by Jinja Regional Referral Hospital staff as well as enhance personal and professional reputations online.

Policy Scope

This policy applies to all Hospital staff and official social media sites that are affiliated to the hospital.

Policy Statements

The following statements shall govern both the usage of official Hospital social media accounts as well as staff social media activity:

a) Hospital Official Social Media Sites and handles:

I. All information shared across the Hospital social media sites should not reference to any biased statements on matters such as politics, religion, race, gender, sexual orientation, inter alia; statements that contain obscenities or vulgarities.

II. Only authorized personnel by the Hospital shall be allowed to make postings on the Hospital official social media sites and handles.

III. Any information shared across the Hospital social media sites shall comply to fair use and comply to Hospital policies in the domains of Conflict of interest and Hospital trademark and symbol protection

b) All staff social media activity shall:

i. Maintain adherence to the overall Hospital Confidentiality agreements and information disclosure

ii. Respect the Laws relating to copyright and other intellectual property rights, defamation, privacy, and other applicable laws

iii. Not malign JRRH staff in an unfavorable light in respect of matters including, but not restricted to, religion, gender, sexual preference, race, nationality or disability

iii. Not share any sensitive staff or student information

Bring your Own Device / Personal ICTs

The Hospital shall allow the usage of personal devices on the Hospital network as long as such complies with the Hospital policies and offers a similar level of protection as specified by committee for ICT. Such usage will be subject to the following:

a) No sensitive or confidential Hospital information shall be stored on such devices.
b) The Hospital shall have the right to investigate/ audit such devices in case of any malicious activity, cybercrime or fraud that affects the Hospital.

Statement of Liability

The Hospital shall not be liable for any errors, omissions, loss or damage, including indirect and/or consequential loss and/or damage claimed or incurred due to any use of any social networking service that does not comply with this Policy or the policies cited herein.

Policy Approach

The Hospital will identify the appropriate unit for maintaining and guiding implementation of this policy.

ICT Services Support or maintenance, development, licensing and Procurement

Introduction

The Hospital management shall ensure the provision of the ICT and assign a central coordination point of contact for all ICT support. The ICT support shall cover all areas under the Hospital ICT Infrastructure including computing devices, software, hardware and implementation of ICT projects and programs and their related technical support. Hospital Systems require on going maintenance and inspection to ensure that they are operating properly; to protect against threats such as attacks, malware and viruses and to protect the integrity and security of information.

Policy Objective

The objective is to define and implement an effective ICT Service Management and Support approach that is aligned to the Vision of the Hospital Strategic Plan where ICT is identified amongst the key components in the support of the Hospital's goals and objectives.

Policy Scope

This Policy establishes organized and coordinated management, responsibility and support of ICT related matters within the Hospital in accordance with the NITA act.

Policy Statement

Roles

a) The Hospital management shall define and implement an appropriate ICT Service Management process and procedure aligned to the goals and objectives of the Hospital

b) Hospital management and / or committee for ICT shall define and implement a Service level contract Model for the provision of ICT services to external clientele.

c) Hospital Management and / or committee for ICT shall mobilize for funds that shall generate resources to improve the welfare of its personnel.

Technology Service Support

The ICT Technology Service Support is any work done by authorized personnel to ensure efficiency, stability and continuity of any ICT service or equipment to ensure it meets its intended user requirements. In line with this, this policy will apply to all Hospital owned ICT applications and devices.

Responsibilities of ICT Tech Services Support personnel

The ICT Services Personnel (system administrators, Computer Lab attendants, ICT technicians, Web administrators) employed by the Hospital within all Units and Departments shall functionally report to committee for ICT. Accordingly, the Hospital shall provide the necessary work tools, safety gear and training for all ICT services support personnel. Accordingly, such personnel shall:

a) Ensure protection of ICT devices to prevent tampering, alteration or theft;

b) Ensure adequate access control exist to safeguard security of systems and information;

c) Provide real time technical support in line with approved ICT procedures for any system, service, device downtime or breach;

d) Ensure installation and configuration of all hardware and software is in line with approved ICT standards;

Policy Approach

The committee for ICT has direct responsibility for maintaining and guiding implementation of this policy.

ICT Skills Capacity Building, Gender and E-Learning Policy

Introduction

There shall be continuous skilling and professional skills development of all staff and students in the hospital on ICTs as an enabler with special interest in gender balance. This will target all users within the Hospital amongst the staff and student community.

Policy Objectives

The purpose of the policy is to:

a) Empower the committee for ICT to:

   i. Carry-out capacity building towards improvement of technical capacities of its staff as per and when need arises;

   ii. Plan and implement capacity building for ICT skills to achieve coherency and efficient utilization of resources.

   iii. Periodically advise the Hospital management on budgetary allocations and make service purchase plans for ICT support and services.

Policy Scope

This policy applies to all ICT related capacity building that supports various functions of the Hospital.

Policy Statements

ICT Capacity Building Assessment

a) The committee for ICT shall:

   i. Undertake a periodic capacity skills assessment to identify knowledge gaps within its technical staff to be able to seek appropriate capacity building interventions.

ii. Coordinate the periodic assessment of existing ICT skills capacity amongst all user groups to be able to identify gaps in partnership with Heads of Departments and units.

Special Needs ICT Usage Policy

Introduction

The provision of ICT services should take into consideration the needs of special user groups to enhance healthcare and teaching. This takes into consideration the visually, motor and auditory impaired user groups. Globally, the development in ICT supports the extension of access to all users.

Policy Objective

The objective of the policy is to define and implement provisions for ICT usage for special user groups within the teaching, learning and research units of the Hospital towards enabling equal access to information and knowledge.

Policy Scope

The policy refers to ICT facilities, equipment and services within all the healthcare service delivery, teaching /learning and research units of the Hospital.

Policy Statements

The following statements govern the implementation of this policy

a) The Hospital shall:

i. From time to time define the appropriate technology aligned to needs of special user groups

ii. provide the provision of staff & end user training

iii. ensure the provision of the appropriate access for special user groups for all Hospital web-based systems

iv. ensure the provision of appropriate digital mechanisms within the Library for special user groups

b) All Hospital Colleges, Departments, Units shall ensure compliance to this policy

c) The Hospital shall ensure the provision of the appropriate access for special user groups for all Hospital web-based systems

Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy.