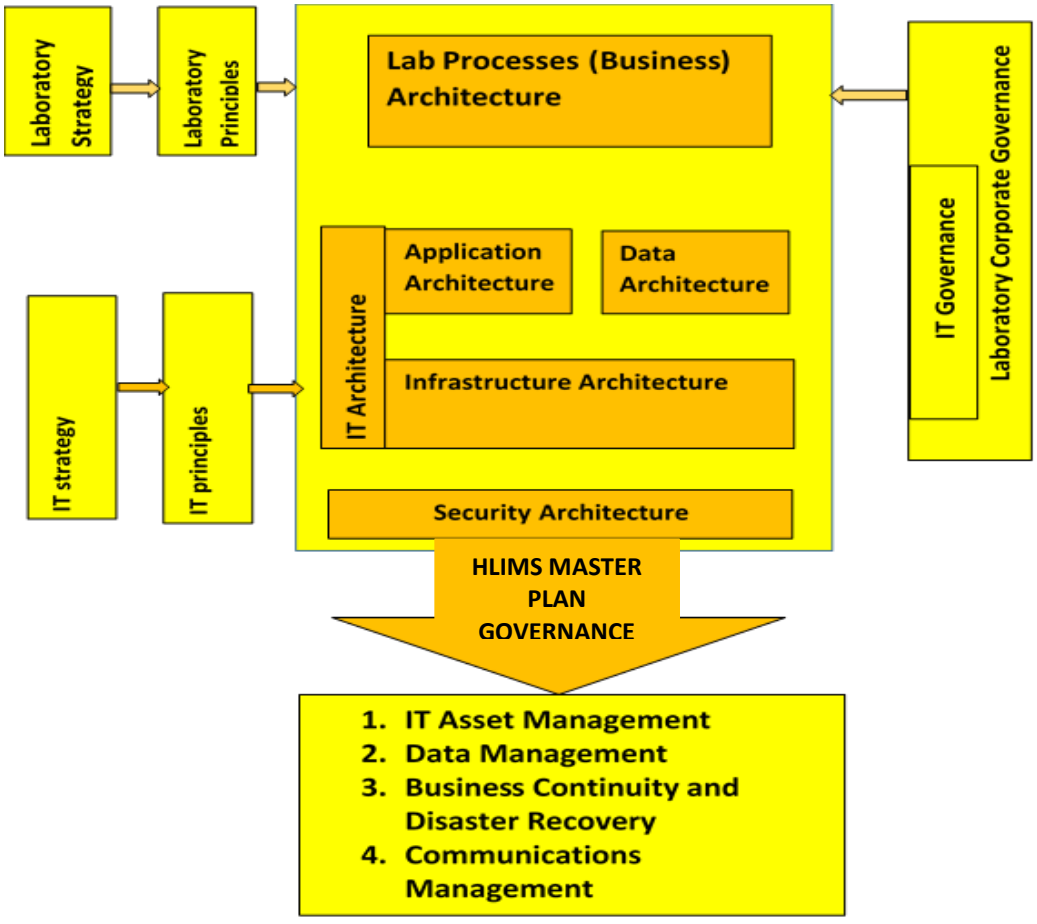
Uganda National Health Laboratory Services

ICT Management Guidelines



The Republic of Uganda

Ministry of Health

Document Version 1.0 - March 2019

LIST OF ACRONYMS

BC	Business Continuity
CPHL	Central Public Health Laboratory
DR	Disaster Recovery
ED	Executive Director
HIPAA	Health Insurance Portability and Accountability Act
HMIS	Health Management Information Systems
ICT	Information Communication Technology
LIMS	Laboratory Information Management Systems
MoH	Ministry of Health
MoICT	Ministry of Information and Communication Technology and National Guidance
NIST	National Institute of Standards and Technology
NITA-U	National Information Technology Authority Uganda
PII	Personally Identifiable Information
PPDA	Public Procurement and Disposal Act
RPO	Recovery Point Objective
RTO	Recovery Time Objective
TOGAF	The Open Group Architecture Framework
UNHLS	Uganda National Health Laboratory Services
UPS	Uninterruptible Power Source
SDLC	Software Development Life Cycle

FORWARD

This Laboratory ICT Guideline is a major milestone in the journey towards quality, responsive, accessible and cost effective laboratory ICT services. A well-developed laboratory program is a fundamental and crucial component of any health system. The use of ICTs is not only a key enabler of direct patient care but also a vital tool in health program monitoring. It therefore requires the necessary attention and well planned investment of resources to realize its function.

These Laboratory ICT Guideline generally align with the goals, and strategies stipulated in the National e-Health policy and strategy for strengthening information technology in the national health services network to facilitate adequate support to the Uganda National Minimum Health Care Package (UNMHCP). In the past decade, laboratory services have seen marked improvement in technology and service delivery. This is as a result of equipment/technology evolution and funding in these areas which been progressively acknowledged by MoH, its partners in health and stakeholders.

Following this guidance in the planning and implementation of ICTs for health services will increase achievement of the expected program benefits towards strengthening laboratory services in both public and private sector. The Ministry of Health is committed to strengthening the coordination and quality of laboratory services to support the Uganda National Minimum Health Care Package. All stakeholders are therefore called upon to examine the laboratory ICT guideline, assess their involvement and thereafter align their present and future SOPs with the guidelines laid out in this document.

.....

Dr. Olaro Charles
Director Clinical and Community Services
MINISTRY OF HEALTH

Acknowledgments

The development of this Laboratory ICT Guideline is a result of contributions and dedicated efforts of the Ministry of Health (MOH), several stakeholders, health development partners and individuals. These parties have been engaged in series of policy reviews, meetings, and workshops, individual as well as institutional consultations to develop these ICT guidelines. UNHLS is grateful for all the support and sacrifice that has been invested for its successful development.

The Division of Health Information, Ministry of Health would like to acknowledge CPHL/UNHLS management and extend its sincere appreciation to the HLIMS team and stakeholders for spearheading the development process, World Health Organization (WHO) Country Office, The United States Centers for Disease Control and Prevention (CDC- Uganda), Clinton Heath Access Initiative (CHAI), African Society for Laboratory Medicine and Implementing Partners

Finally, Ministry of Health is grateful to Ministry of ICT , NITA-U and all those institutions and individuals who have not been specifically mentioned above, but who directly or indirectly contributed to the successful development and finalization of these Laboratory ICT Management Guidelines. The support and contributions from all departments of MOH is appreciated.

.....

Kyozira Carol
Ag. Assistant Commissioner Division of Health Information
Ministry of Health

TERMS AND DEFINITIONS

Data Custodian: refers to an entity (i.e. individual or institution/unit) that is mandated or tasked with the responsibility of storing and archiving data.

Data storage: refers to saving and filing of data on paper based and/or electronic media for future retrieval

Data Backup: refers to storing data in duplicate or multiple locations to allow quick restoration of the original data set in case of any form of disaster.

Data Recovery: refers to the process of restoring an original dataset that was destroyed by some form of disaster.

Data Subject: refers to an entity (i.e. individual or institution/unit) whose attributes are represented in a given data set.

Data User: refers to an entity (i.e. individual or institution/unit) that has a right of access and modification of contents in a given data set.

Data: refers or hand-written or electronic text about attributes of data subjects, or summarized and transformed text about data subjects.

ICT Asset Owner/Holder: refers to an entity (i.e. individual or institution/unit) that is allocated a particular ICT asset in a given period, and is responsibility for ensuring its proper use, security and storage as per the asset manufacturer's instructions or industry standards, best practices and organizational procedures.

ICT Public Assets: This refers to all UNHLS property that is paid for by the organisation to be accessed by anyone or the public.

ICT Services Redundancy: Redundancy refers to the means of duplicating a piece of hardware or software within a system or service so that if one part fails, the others automatically take over.

ICT Services Security: refer to the ongoing and redundant implementation of protections for the confidentiality and integrity of information and system resources to ensure no unauthorized access.

ICT services: The ICT Services described here include all ICT hardware and software, all information systems and services offered by these systems as well as Internet connectivity.

Non-Public ICT Assets: Include all assets procured, donated, created, accessed or transmitted or stored on behalf of UNHLS for official institutional business that is otherwise publicly accessible either though public offices or open records.

Personally Identifiable Information: Any data that could potentially identify a specific individual.

Recovery Point Objective: Is the maximum-targeted period in which data might be lost from an ICT service as a result of disruptive event.

Recovery Time Objective: Is the targeted duration of time and a service level within which an ICT service must be restored after a disruptive event

Risk: The chance of something happening that will have an impact upon set objectives

Contents

1.0. INTRODUCTION

1.1. BACKGROUND TO THE POLICY

CPHL/UNHLS is mandated to coordinate a network of health laboratories in Uganda and provide various reference testing services. The network of health laboratories comprises of various public and private entities, i.e.: Health Centre III laboratories, Health Centre HCIV laboratories, General Hospitals, Regional Referral Hospitals, National Specialized Laboratories; and District-Regional-National coordination teams. CPHL/UNHLS coordinates the laboratory network to deliver services in 14 thematic areas (CPHL, 2016a);

1. Organization and management of the health laboratory system
2. Laboratory services
3. Infrastructure, biosafety and biosecurity
4. Laboratory equipment and supplies
5. Human resources for laboratories
6. Laboratory quality management systems
7. Laboratory information management systems
8. Research and development for laboratory services
9. Point of care testing services
10. Multi-sectorial partnerships and networking
11. Legal and regulatory framework for laboratory services
12. Monitoring and evaluation
13. Financing and accountability for laboratory services
14. Community engagement

Improving service delivery across entities in Uganda's health laboratory network calls for the need to align business strategies in each of the above thematic areas with Information and Communication Technologies (ICTs). Accordingly, one of CPHL's strategic initiatives since 2009 is to establish a robust and integrated Health Laboratory Information System (HLIMS) that can support all the core and support business functions or thematic areas of laboratory service delivery (CPHL, 2010; 2016a). However, establishment of such a complex ICT solution sparks off various strategic, managerial, and operational challenges. To address the strategic challenges, CPHL and its partners developed a master plan as a blue print for guiding decision making and investments on HLIMS establishment in Uganda (CPHL, 2016b). Currently, efforts are ongoing to implement the HLIMS master plan.

However, implementing the HLIMS master plan implies subscribing to governance/managerial and operational challenges that are associated with adopting ICTs within CPHL/UNHLS and across entities that constitute Uganda's health laboratory network. Thus, there is an urgent need to establish mechanisms of preventing governance/managerial and operational issues that may frustrate efforts towards sustainable adoption of ICTs within CPHL/UNHLS and across the health laboratory network.

1.2 SITUATIONAL ANALYSIS AND RATIONALE FOR THE GUIDELINES

At national level and sector level, efforts have been undertaken (and are still ongoing) towards developing a comprehensive legal and regulatory framework for informing the adoption of ICTs and the implementation of electronic services in government service delivery. Table 1 shows existing and/or planned ICT-related policies and other normative compilations at national level and at health sector level.

Table 1. Existing and Planned Policies/Plans/Guidelines/Laws on ICT or Electronic Services

#	At National Level by Ministry of ICT1	#	At Health Sector Level (Ministry of Health)
1	Data protection and privacy bill (2014)	1	E-health policy (2016)
2	Computer Misuse Act (2011)	2	E-health strategic plan (2016)
3	Strategy for Electronic Waste Management (2012)		
4	Information Management Services Policy (2011)		
5	National Information Security Strategy (2011)		
6	Uganda e-government regulations (2014)		
7	Electronic Signatures Regulations (2013)		
8	Electronic Signatures Act (2011)		
9	Electronic Transactions Regulations (2013)		
10	National information and communications technology policy for Uganda (2014)		
11	ICT for disability policy (2017)		
12	IPv6 Policy (2010)		
13	Guidelines for development and management of government websites (2014)		
14	Open Data Policy (2017)		

To realize aspects articulated in the normative documents in table 1, there is need for specific (government) entities to institutionalize concepts therein by adapting them with respect to

[1]Source: http://www.ict.go.ug/laws

peculiarities of the business/operations associated with the mandate of a given sector/entity. In an attempt to holistically and strategically subscribe to the constraints and aspects articulated in the documents listed in table 1, CPHL/UNHLS adopted an Enterprise Architecture approach to develop the HLIMS master plan for guiding decision making in efforts of aligning laboratory business strategies with ICTs. Accordingly, the HLIMS master plan highlights five principles that should be adhered to in the adoption of ICTs within CPHL/UNHLS across the health laboratory network, i.e.:

UNHLS Business Principle: Ensure availability of accurate and timely laboratory data and information to all authorized personnel, towards reliable and responsive laboratory service delivery.

UNHLS Data Principle: Maintain the use of a standard format of a patient laboratory identification number across facility labs and across laboratory information systems, towards data accuracy and reuse.

UNHLS Application Principle: Maintain an up-to-date approved documentation of all existing and planned laboratory information systems, towards minimizing the propagation of isolated or stand-alone laboratory information systems or coordination support systems.

UNHLS Technology Principle: Use reliable and affordable technology solutions that comply with inter (national) e-health guidelines, towards uninterrupted delivery of quality and responsive health laboratory services.

UNHLS Security Principle: To prevent unauthorized individuals or agencies (with or without malicious motives) from accessing laboratory data and services, the use of technologies and data management practices overrides all else.

However, the above strategic principles need to be translated and decomposed into operational guidelines that provide clear guidance on effective governance of routine and periodic ICT practices in specific contexts of laboratory service delivery, in order to avoid issues that cause service delivery mishaps. Since the provision of such detailed guidance on governance and operational issues is beyond the scope of the HLIMS master plan, there is need for a document that gives detailed guidelines on routine and periodic practices that should be institutionalized within CPHL and across the health laboratory network in order to actualize the above five principles.

Accordingly, explicit governance and operational guidance is needed as indicated below:

- To actualize the UNHLS business principle, there is need for communications guidelines
- To actualize the data principle, there is need for guidelines on laboratory data management that can inform both paper based mechanisms and electronic mechanisms of managing data and information on laboratory services.
- To actualize the UNHLS technology principle there is need for guidelines on management of ICT assets (i.e. Hardware and software)
- To actualize the UNHLS application principle, there is need for guidelines on Software Engineering
- To actualize the UNHLS security principle, there is need for a policy on business continuity and disaster recovery.

1.3 GUIDELINES IMPLEMENTATION AND MANAGEMENT FRAMEWORK

1.3.1. Mission, Vision, Values

- **HLIMS Mission:** To support quality laboratory services through an integrated system that innovatively collects, stores, analyses and communicates laboratory information
- **HLIMS Vision:** Quality laboratory information for a productive and healthy Uganda
- **HLIMS Values:**
    - **Integrity** (trust & reliability);
    - **Service Spirit** (availability, responsiveness, proactive planning towards customer satisfaction);
    - **Evidence based decision making** for excellence in planning & operations

1.3.2. Objectives of the Guidelines

- To manage data and information on the delivery of health laboratory services.
- To manage the ICT assets of CPHL/UNHLS and the entities that constitute and support the health laboratory network.
- To manage capability on business continuity and disaster recovery for assurance of health laboratory services.
- To manage the development, acquisition and implementation of software in the laboratory sector
- To manage the communication in the CPHL/UNHLS and the health laboratory network

1.3.3. Scope

This document shall inform ICT-related initiatives and practices within CPHL/UNHLS and in public laboratories on the health laboratory network.

1.3.4 Governance

The Guidelines shall be governed by the UNHLS.

1.3.6 Review of the Guidelines

Management reserves the right to update and amend the ICT Management Policy in accordance with developments in ICT systems, processes and security. The regular review of this operational level ICT Policy shall take place every two years under the coordination of the HLIMS technical working group in collaboration with all stakeholders. Approved changes in the policy within the two-year period shall be retained and applied as administrative notes until the official review of the policy.

1.3.6 Triggers for Review of guidelines

- Standard review is timetabled after every five years
- When a gap has been identified
- When additional knowledge or information has become available to supplement the guidelines.

External factors

- Guidelines are no longer relevant/current due to changes in external operating environment.
- There are changes to laws, regulations, terminology and/or higher-level government policy.
- Changes to funding environment, including requirements of funding bod(y)ies

Internal / organizational factors

- A stakeholder has identified a need, e.g. by email, telephone etc.
- Need for consistency in service delivery across programs and organizations.
- Separate, stand-alone policy or guideline is now warranted
- An unplanned event has occurred, requiring a review to prevent a serious/critical incident in the future

1.3.7 Guidelines Awareness and sensitization

Awareness training and regular updates are to be conducted as per the UNHLS ICT training plan to ensuring compliance to the guidelines herein. Awareness and trainings should then be conducted during employee induction and throughout the work-life span of each staff, contractors and third party relationships to ensure they are able to carry out their responsibilities.

1.3.8 Guidelines Violations and Action

All staff, partners, contractors and third parties are required to observe and comply with these guidelines. Violation to the guidelines herein may be subject to disciplinary and legal actions in accordance with the Public Service Standing Orders, conditions of service and HR manual guidelines.

1.4 Document Format

The guidelines has been designed in accordance to the acceptable International and National policies, standards and guidelines (Normative References). This document generally follows the International Standards Organization (ISO) 27002 (2013) standard framework for information technology security management. The guidelines is also governed by current legislations and acts of parliament.

2.0 IT ASSETS MANAGEMENT (ITAM) GUIDELINES

2.1 Description

This section covers all ICT systems both actively on and off the Uganda National Health Laboratory Services (UNHLS) computer network, which are categorized as hardware, software and infrastructure. It also aims at ensuring that all assets are acquired, used, maintained and disposed-off using proper and authorized procedures. This section of the guideline ensures that all ICT assets in possession of UNHLS are in line with government regulations and other industry standards governing ICT assets management.

2.2 Purpose

To provide guidance for proper ICT Asset classification, inventory management, acceptable use, and protection against loss, damage or liability of these assets for effective and sustained adoption and utilization of electronic information systems at operational level

2.3 Scope

2.3.1 This section of the guidelines shall apply to all ICT hardware, software and infrastructure in form of health information assets described herein including but not limited to; all the desktop computers, laptop computers, servers, smart phones and Tablets, printers, Network equipment (Switches, Routers, etc.), software, data, information systems, Internet, scanners, UPS, data backup facilities, software libraries, manuals, security permissions, website, strategic plans and policies, procedures & standards, data replication, and telephony.

2.3.2 It shall apply to the various Stakeholders including but not limited to; UNHLS staff, implementing partner organizations, District Health offices, health facility management, health facility laboratory staff, service providers and any other users of ICT assets.

2.4 Guideline Controls

2.4.1 Assets Acquisition (Procurement/Donation)

Assets Acquisition in this section of the guidelines refers to process of obtaining assets whether through direct procurement, placement or donation.

i. On acquiring assets, procedures as stipulated in the facility level procurement SOPs shall be followed.
ii. The acceptance or rejection or deferment to reception of the proposed assets shall be in consultation with user department in alignment with current organizational needs, specifications, security, business value, internal maintenance capacity, inter-operability and others.
iii. Acquisition criteria for purchase or lease or donation of laboratory and ICT assets, shall include operational and maintenance costs, installation and training as well as warranty shall be included in the purchase agreement.
iv. All laboratory and ICT equipment acquired for laboratory services shall allow for interoperability and this shall be specified in the acquisition contract.
v. All laboratory and ICT equipment shall be accompanied with manuals that detail information on interoperability with the existing or future laboratory information systems.
vi. Procurement and acquisition of all ICT assets shall be subject to evaluation procedures in line with the PPDA guidelines and shall be adequately communicated and approved by the UNHLS ICT department.

2.4.2 Asset utilization

i. Asset Utilization in this guideline refers to the making practical and effective use of the available assets.
ii. All ICT assets shall be made accessible to the intended users in compliance with the guidance on the acceptable use and quality assurance practices of the organization and laboratory SOPs.
iii. Users shall not access ICT assets without formal authorization or consent as stipulated in the Assets inventory SOPs.
iv. Use of personal gadgets to access organizational resources such as the internet, in the work environment shall be authorized and controlled by the ICT focal person at the facility.

v. Users shall practice secure use of ICT assets and report any incidents on any software, hardware, network breach and any other ICT equipment breakdown.

vi. The ICT department shall ensure that all gadgets are protected using strong authentication methods such as passwords and encryption on various platforms.

vii. Sharable assets such as scanners, printers, modems and copiers shall be assigned based on need and convenience of access, confidentiality and consideration.

viii. The ICT department shall follow a sustainable and manageable ICT equipment maintenance schedule that will cover all ICT equipment deployed within the organization.

ix. Users shall be oriented on user guidelines with respect to associated use of responsibilities communicated through various channels.

2.4.3 Transfer of Assets

Transfer of assets in this section of the guidelines refers to the process that deals with requests, control, approval and delivery of assets from one asset holder to another.

i. Asset transfers from one location/department within the facility to another shall be approved by relevant authority using a Change request form

ii. Transfer of assets from one facility to another shall follow minimum technical standards of packaging and transfer to protect the assets as in ICT asset management SOPs.

iii. All staff are responsible for ensuring that the ICT assets are used and shared in an effective, ethical, and lawful manner.

iv. Unique identification of the transferred assets shall be done following the established facility SOPs

2.4.4 Asset storage

Assets storage here refers to a secure and safe process of storing ICT assets for later use

i. All ICT assets MUST be kept in a secured location; with remote or physical access restricted to authorized staff only.

ii. All off-site storage facilities shall be in a geographical location far from the primary location to protect from the same disaster threat incidents.

iii. All users of ICT assets shall ensure safety of these assets stored in any form. In the event of movement of any ICT asset from one location to another, the new user MUST be oriented on how to transfer, manage and securely store the assets in accordance with security guidelines herein.

iv. All staff and users of ICT assets MUST periodically be reoriented on recommended storage procedures to avoid incident occurrence.

v. All storage practices MUST ensure continuity of business processes to reduce any forms of downtime or bringing work processes to a standstill.

2.4.5 Inventory Management of ICT Assets

Inventory management in this guideline deals with the method of listing ICT assets, to affirm numbers, status and track their use and storage.

i. All the ICT assets shall be recorded and tracked with emphasis on the operational control, user details, geographic location, warranty/licensure, insurance and financial reporting requirements.

ii. All ICT Asset Holders shall ensure that asset inventory with critical information should be recovered in case of a disaster.

iii. The Lifetime of ICT assets shall be reviewed every year by the ICT unit.

iv. All ICT assets shall be verified periodically according to the facility/funding agency guidelines SOPs

2.4.6 Assets Maintenance and Repair

Maintenance and repair in this guideline refers to the process of keeping the ICT assets in good functioning state and restoring the broken, damaged or malfunctioning.

i. All ICT Assets shall be maintained as per the recommendations in manufacturer's manuals, best practices and industry standards.

ii. All ICT assets shall be under a maintenance service contract for optimal functionality, controlled downtime to ensure business continuity.

iii. The ICT unit shall endeavor to perform practicable corrective maintenance as a result of failure to restore an item or asset to its original condition before its write off.

iv. The confidentiality, integrity and availability of the various institutional ICT assets shall be maintained in consideration to their respective asset value and vulnerability

2.4.7 Asset Security

Asset security here refers to the method of safeguarding institutional assets from intrusion, damage or loss.

i. Access to laboratory facilities and ICT assets shall be limited to authorized staff.

ii. All users of ICT assets shall be responsible for the security of all assets under their control to safeguard against theft, damage and unauthorized removal from organizational premises. In case of negligence to these assets procedures shall be followed as stated in the Public Service standing order.

iii. All assets accessible over internal and public networks MUST be secured to maintain and protect their integrity and confidentiality.

iv. Use of passwords, encryption and other protection measures shall be used on all relevant ICT assets.

v. All staff shall receive periodic ICT security trainings as per their respective roles to ensure safe business continuity.

vi. All health facilities and organizations shall establish formal ICT security awareness programs and communicate the guiding frameworks to the various stakeholders.

2.4.8 Asset Disposal

Assets Disposal here refers to the process of writing off of ICT asset that have reached their lifetime

i. Write-off of all ICT Assets shall be in line with the Public Procurement and Disposal Act, and other national regulatory frameworks.

ii. All ICT assets containing storage media MUST be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal

iii. Prior to write-off of an IT asset, a job card should be written to justify the functional status of the IT asset and any remedial actions that were implemented prior to concluding its disposal.

2.4.9 Monitoring and Evaluation

Monitoring and Evaluation of ICT assets will be focused on tracking the adoption and utilization of the ICTs to meet the needs of the respective health programs or activities.

i. ICT implementation, monitoring and evaluation shall be conducted in accordance to established health program goals, standards and plans.

ii. The use of all ICT assets shall be subject to continuous monitoring and evaluation practices to strengthen and enable UNHLS and health programs to respond to the demands for:

   a. Accountability of resources in use

b. Clear basis for decision-making

c. Practical lessons to guide future technological innovations and interventions

iii. Health facilities shall be required to notify UNHLS on up-coming initiatives or projects that will require substantial use of ICTs in order to seek interoperability, harmonization of resource utilization, ensure ethical use of ICT assets for health care and protection of data.

2.5 Roles and responsibilities

Roles and responsibilities here deals with establishing clear authority lines and expectations for various stakeholders.

Role	**Responsibility**
2.5.1 **National level**	a) Endorse ICT Policy guidelines. b) Ensure alignment of the laboratory ICT guidelines with higher-level ICT policies in the Ministry of Health and other government entities e.g. NITA-U. c) Ensure alignment of the laboratory services within MOH-wide IT enterprise architecture, strategic planning and maintenance plans. d) Initiate deployment and early adoption of laboratory information systems (LIS) integrated with other health information systems (HIS) e) Ensure that the data entry and reporting tools in LIS and HIS align with standards of their respective parent paper-based HMIS tools.
2.5.2 **District level**	a) Preliminary planning and budgeting of asset acquisition and equipment maintenance across health facilities. b) Supervise the inter-facility transfer of hardware and other resource tools for ICT implementation. c) Monitor the assets register at health facilities. d) Oversee the effective utilization of ICTs at health facilities for effective health service outcomes as outlined in the M&E needs in section 2.4.9 (Monitoring and Evaluation)

2.5.3 Health facility management level	a) To harmonize the preliminary planning and budgeting of asset acquisition and equipment maintenance for the entire health facility as a unit. b) Maintain the assets register for the whole facility. c) Renewal or purchase of routine accessories, new software for operating systems, office suites and anti-virus software etc. d) IT Capacity planning, costing and recommendation of necessary trainings for the HR e) Provision of administrative support supervision for adoption of ICT initiatives for their proper utilization at health facilities to ensure effective health service outcomes f) Carry out awareness campaigns on new system updates, security threats and incidents to other Users of ICT assets. g) Advises UNHLS and other stakeholders on the end user-needs for software updates and renewal as well as hardware security management. h) Plan and conduct capacity building skills trainings for all Users of ICT assets.

2.5.4 **Lab ICT focal person**	a) Conduct periodic assessments of the ICT assets, the network and ensure reporting for timely maintenance and servicing b) Implement network security practices such as scheduled password changes, review the list of approved users etc. to protect the organization from security incidents c) Coordinate the use of LIS with the various ICT assets within the organization ensuring documentation of technical glitches, failures and related incidents & coordinate the disposal of assets as per the guidance of the asset disposal SOPs. d) Conduct regular preventive system maintenance and monitoring to ensure optimal performance of all assets e.g. troubleshooting to ensure uptime of network services. e) To document and submit error reports to ICT support teams at UNHLS or other support teams requesting remote or direct troubleshooting support e.g using an occurrence/incidence report form. f) To notify the laboratory team & hospital management on up-coming ICT updates, upgrading processes, revisions of assets configurations, patches, and write off obsolete assets through established procedures.
2.5.5 **Users of ICT Assets**	a) Liaise and work with other relevant stakeholders to ensure improved lab service delivery using the ICT assets. b) Report to the ICT focal person incidents, equipment breakdown and malfunction at the earliest time for action. Ensure regular, timely and accurate reporting and promote the use of Laboratory based data to inform planning and management. c) Advises UNHLS and other stakeholders on the end user-needs for software updates and renewal as well as hardware security management.

3.0 DATA MANAGEMENT GUIDLINES

3.1 Description

This section of the guidelines falls under the overall Ministry of Health ICT policy and it's designed to streamline the practice of managing electronic and paper based data within UNHLS and health laboratory network.

3.2 Purpose

3.2.1 The purpose of this guideline is to protect both paper based and electronic data belonging to, or held by UNHLS and the laboratory network. It aims at providing a framework within which the roles and responsibilities of those who manage or use the data and information are defined.

3.2.2 The intention of the guideline is to enable easy access to data and information held by health facilities, to the greatest extent possible, whilst ensuring that electronic data is protected from unauthorised use, access and breaches of privacy.

3.3 Scope

3.3.1 This guideline is designed to deal with all enterprise level data including: health, human resource, assets, finance and accounts data as well as how each of the different data should be stored and accessed.

3.3.2 All staff involved with data management at health facilities will have the necessary and suitable equipment to perform their duties. And all efforts must be taken to ensure that the necessary training and support is adequately provided to all staff.

3.4 Data Management Guideline Controls

Data management shall be an integral part of the health facility operations and its application reviewed and documented on a regular basis by the Data management team.

3.4.1 Classification of Data

a) *Patient Health Data:* This refers to bio and clinical data about a patient

b) *Confidential Data:* Confidential data is data classified as Restricted.

c) *Public Data:* Public data is information that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.

d) *Sensitive Personal Data*: refers to data relating to:

i. Racial or ethnic origin, political opinions or religious and philosophical beliefs of the data subject

ii. Physical or mental health or condition; or sexual life of the data subject;

iii. The record of social behaviors or economic activities done by the data subject;

iv. Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

3.4.2 Data collection and data cleaning mechanisms

i. Data collection shall be done using both paper based and/or electronic information systems that are standardized according to approved HMIS tools.

ii. The data collected shall be securely moved/transmitted from the point of collection to its destination as stipulated by the HMIS guidance.

iii. Automation of data collection processes shall conform to the quality measures and standards stipulated in the software management SOPs.

3.4.3 Data storage, Data backup and Data recovery mechanisms

i. Data shall be stored and backed up using approved procedures and mechanisms as stipulated in approved data backup SOPs.

ii. Data Storage areas/rooms, data centers/server rooms and processing centers shall be setup, managed and secured to only authorized persons.

iii. Data backup and recovery principles shall be in accordance with the needs of Business Continuity and Disaster recovery backup Guidelines.

3.4.4 Data retrieval, Collation, Analysis & Reporting Mechanisms

Access, retrieval, collation and analysis of data shall follow approved procedures as outlined in the facility laboratory SOPs for result and information management.

3.4.5 Dissemination, Feedback, & Use mechanisms

i. Dissemination of data, within or outside the institutions that constitute the health laboratory network shall follow established institutional procedure/protocol with respect to the health facility's result and information management SOPs

ii. The laboratory department shall ensure to protect Personally Identifiable Information (PII) whenever disseminating data.

iii. All Responsible custodians of data shall conduct awareness campaigns on data confidentiality and integrity to all the stakeholders.

3.4.6 Data Archival & Laboratory Business Intelligence

Data archiving is a practice of moving data that is no longer being used for day-to-day operations of an organization.

i. The unit shall establish mechanisms for ensuring that relevant data on laboratory services is properly archived and analyzed to inform strategic decision making.

ii. The unit shall collaborate with key stakeholders to develop SOPs for scanning, storage, archival and destruction of paper based and electronic data on laboratory services in alignment with the National Records and Archives Act.

iii. The data disposal process should ensure that the data is rendered completely unreadable and cannot be accessed or used for unauthorized purposes.

3.4.7 Migration plan (Systems and Data)

i. The shift from paper based to electronic laboratory information systems shall be handled in a phased manner ensuring change management.

ii. Both electronic and paper based laboratory information systems shall be implemented simultaneously at the initial stage until the staff become accustomed to the electronic system.

iii. The laboratory staff shall use the electronic LIS for all the lab processes after they have been accustomed preferably not exceeding 6 months.

iv. The laboratory staff shall fall back to paper based lab information system in case of a confirmed downtime with the electronic system.

v. The laboratory staff shall perform retrospective data entry upon system restoration.

vi. There shall be data migration from one electronic system to another in case of introduction of a new system.

vii. There shall be continuous change management support by the facility management and other support teams.

3.4.8 Safety and Security

In this guideline, Safety refers to the condition of data and files being free from harm or risk, while security refers the quality or state of data and files being free from danger.

i. The ICT unit shall ensure that audit trails and chain of custody for both electronic and paper based data are tracked.

ii. A non-disclosure agreement shall be signed by all parties with access to laboratory data

3.5 Roles and responsibilities

Roles and responsibilities here deals with establishing clear authority lines and expectations for various stakeholders.

Responsible person	Role
Systems administrator	Shall assign access levels and permissions to system users Shall ensure the system is up and running Shall perform data backup and recovery
Data clerk/entrant	Shall organize files and collect data to be entered into the computer Shall report problems with the data Shall accurately enter data into various computer programs Shall keep organization and sensitive (including personally identifiable) information confidential
Data collector	Shall use standard tools to collect data Data collected shall be legible and secured Shall ensure confidentiality of the collected data
Data manager	Shall oversee data entry and perform data verification and validation Shall ensure detailed plans for data collection and collation are in place Shall assist with reporting and data retrieval
Data Analyst	Shall Use statistical techniques to represent data into a more interpretable form such as graphical, tabular dashboard Shall resolving data queries (cross checking of data)
Database Administrator	Shall plan, install, configure and design databases for the organization including backup and data recovery Shall be responsible for the performance, integrity and security of the database

4.0 BUSINESS CONTINUITY AND DISASTER RECOVERY GUIDELINES

4.1 Description

Business Continuity and Disaster Recovery refers to the strategies and actions that provide mitigation, protection or alternative modes of operations for business processes before, during and

after a disaster.

This Business Continuity and Disaster Recovery guidelines provide direction to ensure that UNHLS and all other institutions in the Laboratory Network are able to do the following before, during and after a disruptive event:

i. Process and manage critical information,
ii. Maintain Internet access,
iii. Maintain national and local facility level communications,
iv. Restoration of services and data after a disaster.

4.2 Purpose

The main objective of the guideline is to protect ICT services at UNHLS and all other institutions in the Laboratory Network against disruptions.

Below are the specific objectives:

i. Reduce or mitigate disruptions for day-to-day operations of ICT Services.
ii. Protect data, ICT equipment and other ICT assets from unnecessary failure or loss.
iii. Timely backup and orderly recovery from emergencies for timely restoration of full services to all users.
iv. Identify Business Continuity (BC) and Disaster Recovery (DR) personnel/teams and their roles.
v. Offer Legal protection and due diligence for institutions in the Laboratory Network

4.3 Scope

i. The scope of this section of the guidelines covers all critical ICT services identified by UNHLS.
ii. The Business continuity and Disaster Recover guideline shall apply in all cases of disruption of operations where the critical ICT services are affected.
iii. This guideline applies to all the identified personnel/teams who have vital roles to play in ensuring policy implementation success.

4.4 Guideline Controls

4.4.1 ICT Services Backup

Backup or duplicated copies of data/service shall be stored on different media or additional hardware resources for use to restore to original state after a disaster.

4.4.1.1 Onsite Data/Services

i. Prior to implementation of LIS, all institutions in the laboratory network shall ensure backup capacity of all data/services periodically at an agreed minimum frequency/intervals as guided by the data Back up and Restoration SOPs.

ii. Backups shall be done regularly according to the importance of the information and the acceptable risk as determined in the Back up and Restoration SOPs.

iii. Backups shall be stored in secure locations as per established Back up and Restoration SOPs.

iv. Only authorized personnel shall access the backups for routine viability/validation checkups and restoration.

4.4.1.2 Offsite Data/Services

i. Where critical data/services are hosted offsite, harmonized Back up and Restoration SOPs shall be implemented to ensure security and integrity of data.

ii. Offsite backups must be continually simulated and tested, as per back up and Restoration SOPs, to ensure ability and capacity to restore critical data in the event of a disaster.

4.4.2 ICT Services Recovery

The ICT unit or support team shall establish mechanisms to make the recovery process for data and services hosted both onsite and offsite speedy and accurate with minimal down time.

4.4.3 ICT Services Redundancy

All critical ICT services shall be built with redundancy to ensure resiliency and robustness for availability across the laboratory network.

4.4.4 ICT Services Failure

i. In case of service failure, the ICT unit shall endeavor to perform practicable corrective maintenance as a result of failure to restore an item or asset to its original condition before it is written off.

ii. Following remediation, the ICT unit or support team shall review the facility SOPs to ensure that similar event of a particular service/equipment failure do not reoccur.

4.4.5 ICT Services Security

i. ICT services shall be hosted in a secure physical environment
ii. All critical data at rest and in motion shall be encrypted.
iii. Only authorized personnel shall have access to ICT services

4.4.5.1 ICT Services Change management

ICT Services Change Management in this guideline refers to the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure such as software, information system, LAN or hardware.

4.4.5.2 Succession

The ICT unit or support team shall follow proper hand-over as per the Back up and Restoration SOPs in order to ensure continuity of ICT services when primary responsible staff are absent from station or exiting the role.

4.4.6 Awareness

i. Management and staff shall maintain an appropriate level of knowledge and skills for use of ICT resources to allow for minimal occurrence and low severity of ICT incidents; this shall be done through regular training for basic ICT use.
ii. The ICT focal persons shall coordinate the training on the execution of the procedures that feed into this guideline to ensure accountability and best practices; this shall be done through guideline and procedure awareness workshops.

4.4.7 Compliance Monitoring

The health facility management and district steering committee shall verify compliance to this guideline through various methods, including but not limited to, regular walk-throughs, random checks, business tool reports, internal and external audits as well as feedback to UNHLS from relevant stakeholders.

4.5 Roles and responsibilities

Roles and responsibilities here deals with establishing clear authority lines and expectations for various stakeholders.

Roles	Responsibilities
Business Continuity and Disaster Recovery Steering Committee	It has the role of ensuring the sustained advancement and enforcement of BC & DR and underlying plans throughout

The BC & DR Steering committee will comprise of representatives from key entities across UNHLS/CPHL and all Public Health Laboratories	UNHLS/CPHL and all Public Health Laboratories, by effective, pragmatic means and regularly review the policy as needs arise.
IT Manager (or Team Leader)	Shall be responsible for the documenting, coordinating management decisions on implementation of the Policy and the underlying guidelines. Shall be secretary to the steering committee and ensure all key entities are represented.
Network Administrator	Shall develop and maintain procedures and plans as required under this policy Coordinate execution of the developed procedures
Implementing Partners	Support the execution of the developed procedures
Health facility Staff	All staff and contractors are responsible for contributing to the policy with appropriate guidance, as well as assisting with response and recovery actions following a crisis, emergency or disaster event.

5.0 SOFTWARE ENGINEERING GUIDELINES

5.1 Description

This guideline is designed to help UNHLS software development team to understand their responsibilities with regard to the software development processes.

5.2 Purpose

To direct software engineering processes at UNHLS towards health service delivery.

5.3 Scope

This guideline is limited to the software development processes at UNHLS. These include requirements specification, design, implementation, testing, deployment and maintenance. Any application developed to automate regular processes.

5.4 Guiding Principles

i. Security – All software applications shall have prevention of unauthorized access of all types, including but not limited to hackers, intruders etc.

ii. Testing – All applications developed shall be tested in areas of capacity, performance, security and user requirements.

iii. Intellectual property – All software engineering works (concept, requirement specification, design, software developed, and user manuals) done by employees using UNHLS resources shall be property of UNHLS.

5.5 Guideline Implementation

i. All institution's developers, software users and ICT managers are responsible for understanding and adhering to this guideline.

ii. IT Manager has all responsibility to ensure consistency and standardization of high quality output as per this guideline.

5.6 Guideline Controls

5.6.1 Requirements Gathering

This section directs the procedure for kick-off meetings and understanding of the system which must be realized.

5.6.1.1 All stakeholders shall be identified and involved in the requirements gathering process.

5.6.1.2 All requirements including requested changes shall be collected, documented and signed off/approved.

5.6.2 Development

This section describes the guidelines that will govern and guide the development of any software

5.6.2.1 All software development shall be done using languages and frameworks approved/allowed by the institution.

5.6.3 All development shall be done using approved IDEs

5.6.3.1 The coding standard for the software development shall follow the same standard (adopted by institution) every time a need of development is identified.

5.6.3.2 All software developed shall be done with reuse in mind and software engineering principles (separation of concerns, modularity, consistency and abstraction, anticipation of change, generality and incremental development).

5.6.4 Testing

5.6.4.1 All applications developed shall be tested using the SDLC before they are deployed for use.

5.6.5 Maintenance and Support

i. Once an application is in use, any required changes shall be documented and approved.

ii. Minor bug fixes may not require a new version update while major upgrades shall be implemented in a different version.

5.6.6 Change Request and Approval

The end users or IT support teams shall address change request, which is different from the specifications requirements, to appropriate key stakeholders such as health facility

administration and UNHLS to ensure a satisfactory implementation of the change, and communicate the result of the change to all stakeholders.

5.6.7 Security

5.6.7.1 All software developed shall be deployed on secure servers and networks.

5.6.7.2 All data in the application shall be protected using the UNHLS data backup guideline and the National data protection act.

5.6.8 Discontinuation

This section deals with the steps and care that must be taken in the event that a system is not to be used any more.

5.6.8.1 Before a system is decommissioned (taken out of use), all data in the systems shall follow the UNHLS data management guidelines.

5.6.9 Intellectual Property

5.6.9.1 All software developed, documents and tools created during the SDLC process shall remain a property of UNHLS.

5.7 Roles and Responsibilities

Role	**Responsibility**
Systems administrator	Ensures systems are deployed on secure servers and accessed by authorized users
Team lead	Oversees the guideline implementation
Developer	Designs and develops systems which meet defined requirements
Systems Analyst	Gathers and documents all system requirements
Tester	Verifies and validates that the system conforms to the documented requirements

6.0 COMMUNICATION GUIDELINES

6.1 Description

This section of the guidelines falls under the overall Ministry of Health ICT policy and it's designed to streamline the practice of managing communication within CPHL/UNHLS and other institutions.

6.2 Purpose

CPHL/UNHLS is committed to effective dissemination, receipt of information and communication within the organisation and other stakeholders. This section provides guidance to CPHL/UNHLS and other institutions in developing and implementing communication strategies. This guideline applies to all staff, volunteers, and interns. It encompasses:

i. Reason for communication
ii. Communication tools and mechanisms
iii. Parties involved
iv. Liaison with the media

6.3 Scope

This guideline provides guidance on:

i. Feedback and complaints from stakeholders
ii. Privacy and confidentiality
iii. Partnerships and relationships with external parties
iv. Management of the organisation's information

6.4 Principles

i. Communication systems and equipment shall be used only for the purpose of achieving the organisation's objectives.
ii. Communication channels shall be clear and consistent within the organisation for effective operations.
iii. Communications shall be presented in an official language.
iv. External communication, including the media shall align with the organisation's strategic objectives.

6.5 Guideline controls

6.5.1 Purpose of Communications

Communications are undertaken not for the sole purpose of information distribution and receipt, but to be used to assist and support the achievement of an organization's strategic objectives as stipulated below;

i. To increase awareness of the organisation's vision and mission
ii. To share knowledge with stakeholders
iii. Share knowledge internally for effective organisational management
iv. Increase the profile of the Laboratory sector.

6.5.2 Types of Communications

6.5.2.1 Outgoing Communication

Outgoing communication is information and knowledge that is initiated, developed and distributed by the organisation for an external audience.

CPHL/UNHLS provides outgoing communications to Consumers, engaged and potential consultants, Partner organisations, Ministries, departments and agencies, Research and academic institutes, Media.

6.5.2.2 Incoming Communication

Incoming communication is information and knowledge that is sought and/or received from an external source to the organisation. Incoming communication supports the institution in achieving its goal, strategic plan and provision of services to consumers.

6.5.3 Mechanisms and Tools used for Communication

6.5.3.1 Outgoing Communication

A range of mechanisms and tools are used to distribute outgoing communication.

i. CPHL/UNHLS website
ii. Newsletter
iii. Media communication
iv. Conference, forum and meeting representation
v. Stakeholder meetings

6.5.3.2 Internal Communication

A range of mechanisms and tools are used for internal communication.

i. Staff, Team and Project Meetings
ii. Board Meetings
iii. Work-Plan and Review Meetings
iv. Email and Electronic Calendars

6.5.4 Use of official Internet, Email and Phone

i. All CPHL/UNHLS staff, volunteers and interns shall use the organisation's communication systems and equipment for official purposes only.
ii. Staff, volunteers and interns shall comply with guidelines when using the UNHLS communication systems.
iii. Using the organisation's computer resources to seek out, access, store or send any material of an offensive, obscene or defamatory nature is prohibited and may result in disciplinary action.
iv. All internet activities shall be monitored.

6.5.5 Record Keeping

All documents bearing the institution name and/or logo, including digital and electronic materials, must be saved in the electronic and hard copy filing systems, as per the Records Keeping SOP.

6.6 Roles and Responsibilities

Role	Responsibility
Top Management	• Endorse communications SOPs. • Monitor compliance with communications SOP. • Contribute to internal and external communication strategies and activities. • Endorse media releases prepared by other staff
Senior Management	• Contribute to internal and external communication strategies and activities.

	• Actively contribute/ write articles and collate items of interest for CPHL/UNHLS' communications. • Oversee production of external communications.
Website Administrator	• Maintain operations of the website, and other promotional materials • Shall publish endorsed content by Top Management • Update content of the communications database. Production of the newsletter
Communications specialist	• Produce press releases and manage public events • Liaise with media, including developing and responding to media releases • Offer technical advice on communication to the Top Management • Review information before publishing
Staff	• Compliance with Communications guideline. • Contribute to internal and external communication strategies and activities. • Contribute/ write articles and collate items of interest for organization's communications.

7.0 References

Guidelines for Computer, Internet, Email & Phone Use

Information Management Policy

Integration Policy Privacy and Confidentiality Policy

Project funding agreements

Public Procurement and Disposal Act

Ministry of Health ICT Policy

ISO 27001/27002

Guidelines and Standards for Acquisition of IT Hardware & Software for MDAs

Records and archival management act

E-Health policy

USA HIPAA law

Data Protection and Privacy bill

The national ICT Policy

The Computer Misuse Act

HMIS Manual

Health Information systems Operating Procedure

ISO 22301: 2012: Business Continuity Management Systems Requirements

BS 25999: British Standard for Business Continuity Management Systems

NIST Contingency Planning for IT Systems

SANS: Disaster recovery policy plan guidelines.

Guidelines for Operation, Usage and Management of IT Infrastructure in MDAs & Local Government

Standards for Structured Cabling for Government MDAs.

APPENDIX 1: SERVICE TIERS AND CORRESPONDING RECOVERY OBJECTIVES

Within UNHLS, the following levels of disaster recovery Applicability apply

Tier	Applicability	Recovery Objective
1	A Tier 1 system is any critical system necessary to support the delivery of primary services by ICT Services. Primary services are defined by the e-services manager and supporting systems are identified through Corresponding analysis.	All Tier 1 systems are fully resilient and redundant across dual-data centers. The design recovery time objectives (RTO) for Tier 1 systems are a maximum of 24 hours. The minimum essential services for all critical systems are identified and documented. Significant projects and changes associated with these services must have documented and tested contingency plans- e.g. back out plans, contingency services, extended change outage windows.
2	A Tier 2 system is any other non-critical system operated or managed by ICT Services as a production system for CPHL's operations.	Tier 2 systems have a design maximum recovery time objective (RTO) of 72 hours, and all minimum essential services are identified to ensure efficient recovery. Minimally, all Tier 2 data shall be recoverable from remote offline backup storage media, and where necessary and feasible, full systems shall be backed up. Significant projects and changes associated with these services must have documented contingency plans.
3	Tier 3: Non ICT Services Incidents	These are incidents, which involve the loss of use of office facilities by administration or other organization staff through a significant unplanned event. In such events ICT services facilitate the provision of short term or temporary facilities to accommodate such staff in conjunction with Buildings and Services

APPENDIX 2: CHANGE REQUEST FORM

Ministry of Health	Change Request Form	Form Number: MOH/ICT/01

This Change Request Form must be completed to request approval for a significant business, technical change to the approved requirements in the original Plan. Please attach any supporting documentation that will be helpful for the approval process.

1. REQUEST DETAILS

Request No.	Name of Requester	Dept./Project Name	Designation	Contact	Signature

2. CHANGE DETAILS

Description of Change			
Reason for Change			
Date of Request		**Date Needed**	

3. CHANGE JUSTIFICATION

Priority	**Urgent**	**High**	**Medium**	**Low**
Intended outcome(s)				
Expected benefit(s)				

CHANGE APPROVAL RESPONSE DETAILS
(To be completed by approval Officer)

Approved (Yes/No)	Decision date	Decision made by	Decision reason	Resulting Action

3.) CHANGE APPROVAL TEAM– DECISION

Decision	☐ Approved	☐ Approved with Conditions	☐ Rejected	☐ More Info
Decision Date	[mm/dd/yyyy]			
Decision Explanation	[Document the CAT's decision]			
Conditions (Implementer and Date scheduled for change)	[Document and conditions imposed by the CAT]			
Approval Signature	[Approval Signature]		**Date Signed**	[mm/dd/yyyy]

CHANGE VERIFICATION DETAILS
(To be completed by Head of ICT)

Verified (Yes/No)	Verification date	Verified by	Signature

APPENDIX 3: ASSET ALLOCATION/TRANSFER FORM

Ministry of Health	Asset Allocation/Transfer Form	Form Number: MOH/ICT/02

Please fill this form if you intend to transfer an Asset from one location to another within Ministry of Health or externally

1. ASSET DETAILS

Asset Name	Model	Serial no.	Engraved No./Batch No.	Reason for Allocation/Transfer

2. ALLOCATION/TRANSFER DETAIL:

Current Department: _____ **Current Location:**_____
New Department: _____ **New Location:**_____
Date Transferred: *Month*_____ *Day*_____ *Year*_____
Briefly explain why asset is being allocated/transferred:
_____
_____
_____

3. AUTHORIZATION DETAIL:

Authorized by:

HoD: _____
Signature: _____
Date: _____

Receiving Officer:
Name: _____
Signature: _____
Date: _____

NB: The form should be filled in duplicate.

APPENDIX 4: DATA BACKUP LOG

Year_____ Month_____

Date	Daily backup	Weekly backup	Monthly back up	*Initials*
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				

Reviewed by: _____*Date:* ____/___/_____