REPUBLIC OF KENYA

HEALTH SECTOR ICT STANDARDS AND GUIDELINES

Ministry of Health

June - 2013

`

HEALTH SECTOR INFORMATION COMMUNICATION TECHNOLOGY STANDARDS AND GUIDELINES

June 2013

`

Table of Content

`

`

`

`

Acronyms

CAPTCHA: **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part
CCTV: Closed Circuit Television
COTS: Customized Commercial Software
CPE: Continuous Professional Education
DeG: Directorate of e-Government
DHIS: District Health Information System
DICOM: Digital Imaging and Communications in Medicine
DMZ: Demilitarized Zones
DR: Disaster Recover
EHR: Electronic Health Record
EMR: Electronic Medical Record
ERP: Enterprise Resource Planning
E-Waste: Electronic Waste
FOSS: Free and Open Source
HIS: Health information System
HL7: Health Level 7
HRD: Human Resource Department
ICT: Information and Communication Technology
ID: Identification
IS: Information System
ISO: International Organization for Standardization
IT: Information Technology
LOINC: Logical Observation Identifiers Names and Codes
M & E: Monitoring and Evaluation
MDA: Ministries, Departments and Agencies
MFL: Master Facility List
MOH: Ministry of Health
NOC: Network Operations Centre
OEM: Original Equipment Manufacturer
OSS: Open Source Software
PACS: Picture Archiving Communication System
PC: Personal Computers
PDA: Personal Digital Assistant
PIN: Personal Identification Number
SAN: Storage Area Network
SDLC: Software Development Life Cycle
SDMX: Statistical Data and Metadata Exchange
SNOMED: Synchronized Nomenclature of Medicine
SOP: Standard Operating Procedure
SWOT: Strength, Weakness, Opportunity, Threats
TCP: Transmission Control Protocol
UPS: Uninterruptible Power Supply
USB: Universal Serial Bus
UTP: Unshielded Twisted Pair

`

VPN: Virtual Private Network
WAN: Wide Area Network

`

FOREWORD

The Ministry of Health recognizes the value of using ICT as a means of enhancing efficiency in the delivery of health services. ICT has the potential to impact upon almost every aspect of the health sector. In public health, information management and communication processes are pivotal, and are facilitated or limited by the available information and communication technology. In addition, beyond the formal health sector, the ability of impoverished communities to access services and engage with and demand a health sector that responds to their priorities and needs, is importantly influenced by wider information and communication processes, mediated by ICT.

The implementation and utilization of ICTs in healthcare in the country initially adopted a diversified approach, where the implementers worked in a relatively autonomous environment without any reference to a common set of standards and guidelines. This approach has led to duplication of efforts, lack of interoperability, and inappropriate use of ICT resources thereby making it difficult to effectively and efficiently use ICT for healthcare service delivery.

As the Ministry of Health increasingly embraces ICT in its service delivery, it is becoming more important that a common approach based on recognized best practices is taken. The Ministry recognizes the need for a consistent approach to the use of ICTs and thus the formulation of this ICT Standards and Guidelines Document to provide citizens with high quality, consistent, accessible and useable services.

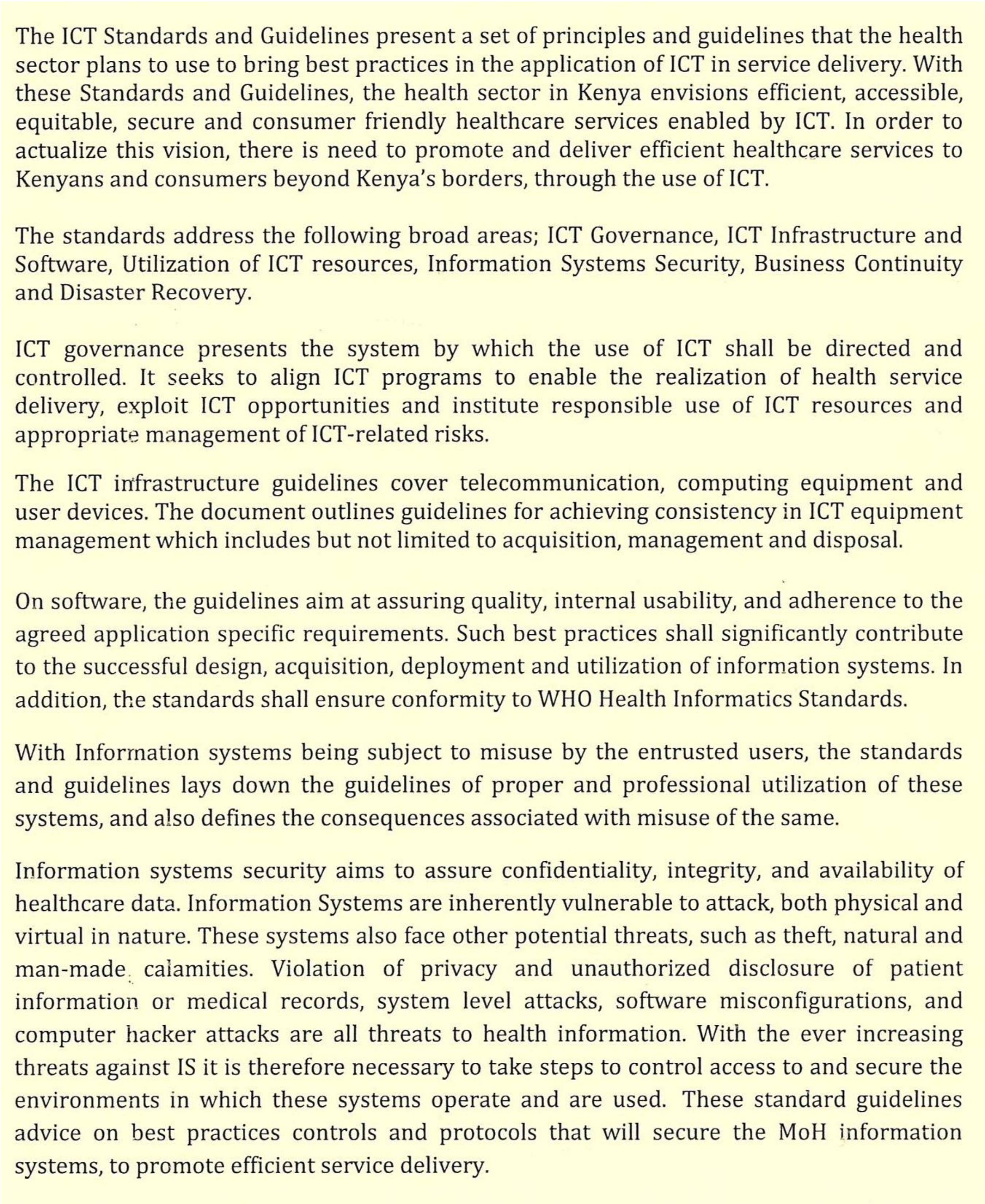
The standards set out in this document shall be applied in the health sectorin the usage of ICTs by those involved in offering services or information to the public. This document provides guidance and a consistent approach across the health sector in establishing, acquiring and maintaining current and future information systems and ICT infrastructure.

This document was developed through a participatory process involving all stakeholders in health including government ministries/agencies and development partners, andis based on internationally recognized best practice principles and was done in consultation with a vast array of subject experts and interest groups, with input from all Government MDAs.It shall be used in accordance with the Ministry of Health Strategy and borrow from e-Government Standards and shall be reviewed and updated regularly.

It is our sincere hope that all the actors in health in Kenya will rally around these guidelines to ensure that we all steer the country towards the acceptable use of ICT.

…………………………………………………	…………………………………………………
Ms. Mary Ngari, CBS	Mark K. Bor, CBS
Permanent Secretary	Permanent Secretary
Ministry of Medical Services	**Ministry of Public Health and Sanitation**

PREFACE



The ICT Standards and Guidelines present a set of principles and guidelines that the health sector plans to use to bring best practices in the application of ICT in service delivery. With these Standards and Guidelines, the health sector in Kenya envisions efficient, accessible, equitable, secure and consumer friendly healthcare services enabled by ICT. In order to actualize this vision, there is need to promote and deliver efficient healthcare services to Kenyans and consumers beyond Kenya's borders, through the use of ICT.

The standards address the following broad areas; ICT Governance, ICT Infrastructure and Software, Utilization of ICT resources, Information Systems Security, Business Continuity and Disaster Recovery.

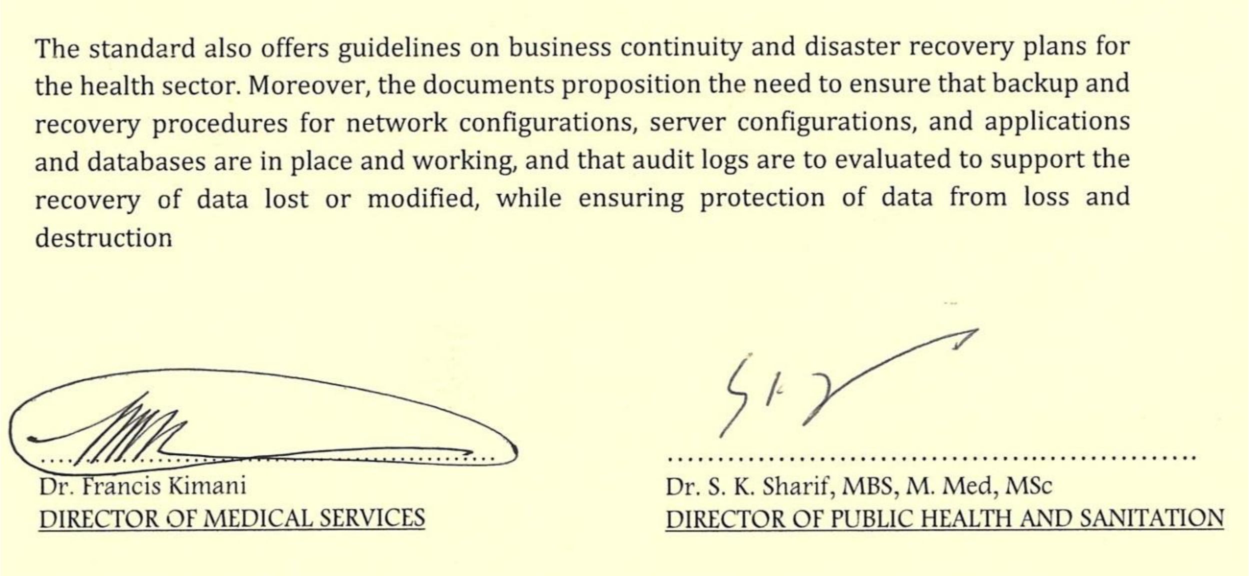
ICT governance presents the system by which the use of ICT shall be directed and controlled. It seeks to align ICT programs to enable the realization of health service delivery, exploit ICT opportunities and institute responsible use of ICT resources and appropriate management of ICT-related risks.

The ICT infrastructure guidelines cover telecommunication, computing equipment and user devices. The document outlines guidelines for achieving consistency in ICT equipment management which includes but not limited to acquisition, management and disposal.

On software, the guidelines aim at assuring quality, internal usability, and adherence to the agreed application specific requirements. Such best practices shall significantly contribute to the successful design, acquisition, deployment and utilization of information systems. In addition, the standards shall ensure conformity to WHO Health Informatics Standards.

With Information systems being subject to misuse by the entrusted users, the standards and guidelines lays down the guidelines of proper and professional utilization of these systems, and also defines the consequences associated with misuse of the same.

Information systems security aims to assure confidentiality, integrity, and availability of healthcare data. Information Systems are inherently vulnerable to attack, both physical and virtual in nature. These systems also face other potential threats, such as theft, natural and man-made calamities. Violation of privacy and unauthorized disclosure of patient information or medical records, system level attacks, software misconfigurations, and computer hacker attacks are all threats to health information. With the ever increasing threats against IS it is therefore necessary to take steps to control access to and secure the environments in which these systems operate and are used. These standard guidelines advice on best practices controls and protocols that will secure the MoH information systems, to promote efficient service delivery.



The standard also offers guidelines on business continuity and disaster recovery plans for the health sector. Moreover, the documents proposition the need to ensure that backup and recovery procedures for network configurations, server configurations, and applications and databases are in place and working, and that audit logs are to evaluated to support the recovery of data lost or modified, while ensuring protection of data from loss and destruction

Dr. Francis Kimani
DIRECTOR OF MEDICAL SERVICES

Dr. S. K. Sharif, MBS, M. Med, MSc
DIRECTOR OF PUBLIC HEALTH AND SANITATION

`

ACKNOWLEDGEMENTS

The realization of these ICT Standards and Guidelines has been achieved through tremendous efforts and commitment of various individuals and organizations.
We would like to acknowledge the contributions of Hon. Prof. Peter Anyang' Nyong'o, former Minister for Medical Services , Hon. Beth Mugo, former Minister for Public Health and Sanitation whose leadership ensured that the document was realized.
The contributions of Hon. Dr. O. Gesami, former Assistant Minister for Public Health and Sanitation and Hon. Samwel Kazungu Kambi, former Assistant Minister for Medical Services are highly appreciated.

Special thanks go to our Permanent Secretaries Mr. Mark Bor and Ms. Mary Ngari whose enormous support and guidance led to the finalization of the document.
Dr Francis Kimani, Director of Medical Services and Dr S. Sharif, Director, Public Health & Sanitation ensured that there was full participation of Ministry staff and stakeholders in the entire process. The personal support and contribution of Dr. Samuel Were was critical from the inception to the realization of the Standards and Guidelines.

The support and contributions of Dr. Katherine Getao, the ICT Secretary, ensured that ICT Staff from the Directorate of e-Government were always available in the entire development process.

The process received tremendous technical and financial support from our partner through the US President's Emergency Plan for AIDS Relief (PEPFAR) cooperative agreement between CDC and Futures Group. Special thanks go to Ms. Anne Barsigo, the Chief of Party, Mr. Joshua Oiro, Ali Karisa Juma and Mr. Gitonga Mwenda of Futures Group for their unrelenting support throughout the entire process.

Special thanks also go to Mr. James Njiru and Mr. Edwin Kemboi, the heads of ICT in the Ministry of Public Health and Sanitation Ministry of Medical Services respectively for their steadfast leadership and coordination in the realization of this document. Appreciation goes to Ms. Rachael Wanjiru , Mr. Nicholas Ngari and Mr Benard Ajwang for their active participation in the process.

As we may not be able to mention everyone, we would wish to sincerely thank everyone including all the heads of departments and divisions, members of staff and health sector stakeholders who in one way or another participated in the realization of the ICT Standards and Guidelines, 2013.

`

INTRODUCTION

BACKGROUND

Article 43 (1) (a) of the Kenyan constitution guarantees that every citizen has the right— to the highest attainable standard of health, which includes the right to health care services, including reproductive health care. The National Health Policy further identifies specific tenets of health systems focus areas that need to be strengthened to enable response to this constitutional requirement. The National health strategic plan specifies ICT as a catalyst to attaining efficiency in multiple facets of the above areas.

As the Health Sector deepens the devolution of health services there is the inherent risk of adopting a diversified approach, where ICT implementations may occur in a relatively autonomous environment without any reference to a common set of standards and guidelines. This will in turn present challenges in integration at inter and intra-county as well as across the two levels of government.

Therefore as departments responsible for Health between the two levels of Government, increasingly embrace ICT in service delivery, it is therefore necessary to have a common approach based on recognized best practices and standards.

RATIONALE AND SITUATION ANALYSIS

ICT capacity in the Public Health Sector has grown as demonstrated by implementation of various HIS systems such as DHIS, MFL and EMR among other systems. Alternately, ICT infrastructure has improved through the installation of Local Area Networks and a data centre at the ministry national level. These ICT investments have led to improved service delivery and enhanced information exchange within the health sector.

The new challenge currently experienced in the delivery of ICT service is to ensure consistency in ICT implementation and harmonization of health sector system requirements.

The challenges experienced by ICT service area include low level of capacity in terms of technology, centralization of the ICT capacity at the national level, lack of information systems integration, state of facilities and infrastructure at sub national and health facilities.

The objective of these ICT standards and guidelines is to ensure consistency in ICT initiatives and management so as to achieve efficiency thereby improving healthcare delivery.

`

STANDARD AND GUIDELINES STATEMENT

The Ministry of Health will continuously enhance its organizational capacity by adopting modern technologies and skills development. These standards will provide guidance to both levels of government, to ensure that ICT resources are optimally utilized in order to achieve efficiency in healthcare delivery.

The standards promote principles that guide implementation of robust ICT infrastructure, Information systems, support services and operational capacity.

AUTHORITY

The standards and guidelines derive the authority from:

(i) Health and other relates Acts, Laws of Kenya;
(ii) Kenya Communications Act 2009;
(iii) E-Government Strategy ;
(iv) The National ICT Policy

Any other relevant legal provision and Government policies that may come into force after initial implementation of these standards and guidelines

VISION STATEMENT

To provide leading edge, integrated ICT solutions derived from identified strategies based on defined technologies and processes for effective and efficient health care delivery and operating excellence

MISSION STATEMENT

To maximize MoH ability to realize its Mission – innovatively, creatively, efficiently, and effectively – and to add value to health care delivery services in order to improve health and well-being of Kenyans.

OBJECTIVE OF THE MOH ICT STANDARDS

Specific objectives

- Support the development, implementation and maintenance of ICT Systems in MOH;

- Enhance information security of MOH ICT systems.

- Promote efficient and effective operations and usage of ICT systems within the MOH;

`

- Encourage innovations in technology development, use of technology and general work flows within the MOH;
- Facilitate the development of ICT skills to support ICT systems in the MOH;
- Promote efficient communication among the MOH's staff and stakeholders;
- Promote information sharing, transparency and accountability within MoH and towards the general public and other stakeholders.

Scope

The ICT standards shall apply to the MOH and its stakeholders in relation to all MOH ICT related operations.

Key Principles

This standard shall be guided by the following key principles:

(i) Mainstreaming of ICT in the Ministry
(ii) Integration of ICT systems
(iii) Adherence to best practices & policies
(iv) User, customer, patient satisfaction

Roles and Responsibilities

The overall responsibility of implementing this standard will lie with the Principle Secretary in collaboration with ICT Governance Committee which will be responsible for the overall strategic management of ICT resources in the Ministry. The committee will draw representation from heads of departments and the head of ICT being secretary. The committee will be responsible for oversight, enforcement and review of the standards and the initiation of ICT projects.

`

ICT GOVERNANCE

ICT governance is the system by which the use of ICT is directed and controlled. It evaluates and directs the use of ICT to support the organization achieve its goals.

Governance of ICT aims to direct ICT endeavors to accomplish the following objectives:

(i) Align ICT programs to enable the realization of health service delivery

(ii) Enable exploitation of the ICT opportunities to maximize benefits for the health service provision;

(iii) Institute responsible use of ICT resources; and

(iv) Institute appropriate management of ICT-related risks.

ICT Governance Committee

The committee will be composed of Principle Secretary as the Chair or a designated representative. Other members will be heads of departments, representatives of ICT development partners in the health sector. The head of ICT shall be the secretary of the committee.

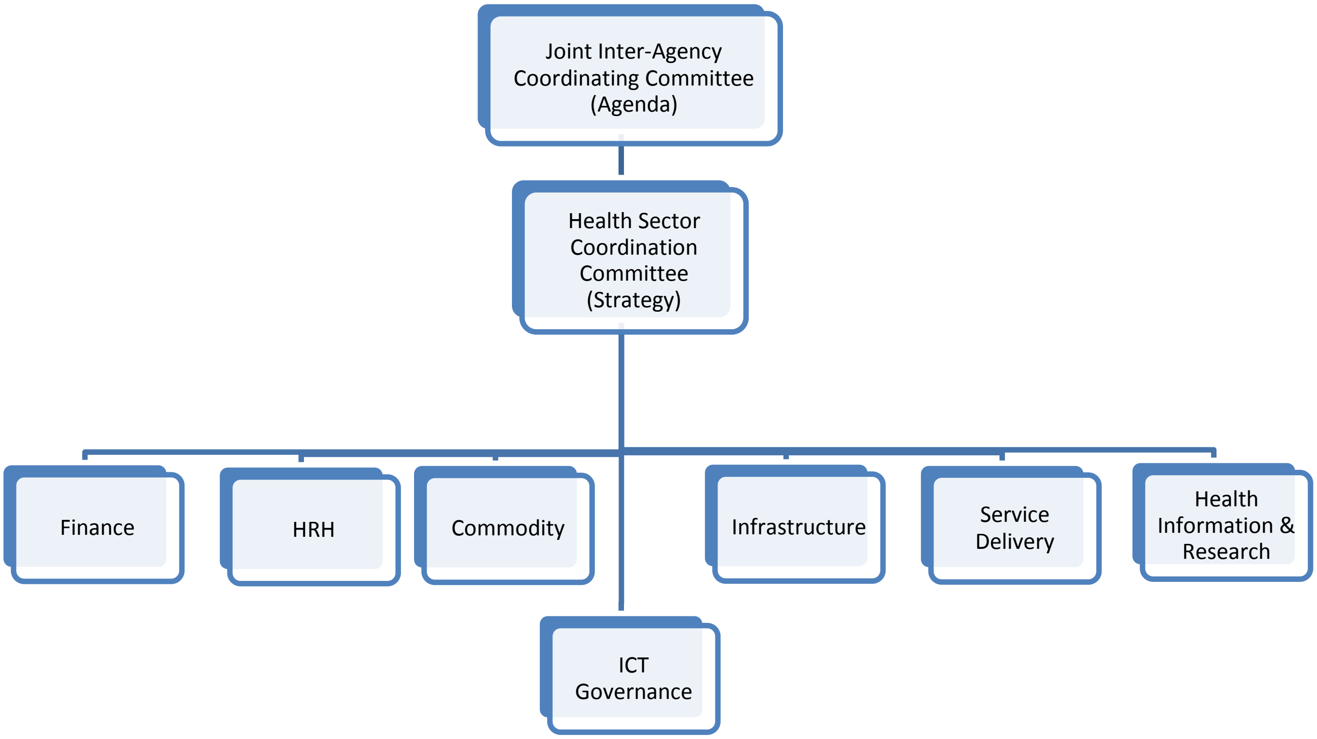
The ICT Governance Committee is necessary to formulate and advance the programs of the ICT Division within the health sector. The committee will give direction for National and County ICT programs

The roles of the ICT Governance Committee shall include but not limited to:

- Review and provide advice on ICT investment priorities in the health sector;
- Mobilization of resources for ICT investment in the health sector;
- Provide ICT strategies, policies and standards;
- Provide guidelines and policies for technical ICT programs
- Provide general advice and guidance on ICT matters in the health sector;
- Raise awareness on the strategic value of ICT in the health sector; and
- Promote information sharing on ICT programs in the health sector

The placement of this committee in the health sector governance structure is as indicated below:

`


Joint Inter-Agency Coordinating Committee (Agenda)
Health Sector Coordination Committee (Strategy)
Finance
HRH
Commodity
Infrastructure
Service Delivery
Health Information & Research
ICT Governance

Technical Committees

The Head of ICT Division will constitute ad-hoc committees to deal with matters of innovation, technical advice, disposal/decommissioning, and inspection of ICT Systems, among others. Where cross-cutting issues of ICT are involved such as evaluation, the Head of ICT will appoint representatives as appropriate. Such committees will have various roles dependent on the reason for their constitution.

Organization of the ICT Division

The ICT Division head will be responsible for leadership, administration and management of the ICT Division.

The ICT Division will be organized to deliver ICT services for MOH along these areas:

- Systems administration (server admin, email admin, dB admin)
- Network administration
- Webmaster and web systems admin
- Information Security
- User support (help desk services, etc.)

`

ICT INFRASTRUCTURE STANDARDS AND GUIDELINES

The ICT Standards and Guidelines recognize that ICT comprises both equipment and the software that run them. The following section specifies IT equipment standards and guidelines.

The ICT equipment standards and guidelines stipulated herein shall apply and be used in the procurement, management, maintenance and disposal of all ICT equipment.

General IT Equipment Guidelines

The following guidelines shall be observed by the Ministry of Health and its agencies:

a) MOH computing environment shall endeavour to be technology-neutral.
b) Information Technology shall aim at improving service delivery by MOH.
c) IT service delivery by MOH shall leverage current and new technologies.
d) Guidelines on relevant ICT infrastructure, software, and applications shall be developed and reviewed from time to time for adoption and implementation.
e) New technologies, products or services shall take cognisance of existing infrastructure, platform and prevailing guidelines.
f) Advances in technology, services and embedded applications shall be identified, adopted and implemented where possible.

ICT equipment management guidelines

These guidelines shall direct MoH in their use and management of all ICT equipment not limited to personal computers, desktops, workstations, laptops, printers and peripheral devices. This also includes telecommunications equipment such as routers, switches, hubs and other network devices.

The ICT equipment management guidelines aim to:

a) Guide procurement and disposal of ICT equipment
b) Ensure MoH receives value for money on ICT equipment
c) Ensure compatibility and interoperability both within and across MoH.
d) Ease maintenance
e) Ensure cost effective use of ICT equipment.
f) Ensure consistency in ICT equipment performance
g) Maximize the equipment functionality
h) Improve end-user performance and experience

Roles and Responsibilities

The ICT unit shall develop and update minimum specifications of all categories of ICT equipment on a regular basis in conjunction with the Directorate of e-Government or a designated agency mandated by Government to manage ICT. Specification of ICT equipment aims to ensure that appropriate equipment is acquired that is fit for purpose, cost effective, and has extended useful life.

The ICT unit shall be charged with the responsibility of installation, upgrade, support and maintenance of the ICT equipment.

The Head of ICT Unit shall enforce these standard specifications and give advice where specifications above the minimum are required.

While developing specifications, the ICT unit shall take into consideration the end user requirements.

The Supply Chain Management Unit shall liaise with the ICT unit to procure quality ICT equipment and consumables in a timely manner.

End-users shall take care of any ICT equipment allocated to them. Any issues arising in the course of usage of the equipment shall be brought to the attention of the ICT Unit.

The ICT unit shall also sensitize end-users on the proper usage of equipment in their custody.

Procurement

Procurement of ICT equipment shall be done according to relevant government procurement regulations and statues in force at the time.

Procurement of ICT equipment shall be channelled through the Head of ICT Unit who shall be responsible for the preparation and issuance of all technical specifications for the equipment, as well as ensuring that the guidelines stipulated herein are adhered to.

Due diligence shall be undertaken by ICT Unit before taking the decision to acquire ICT equipment. Such equipment must be deemed necessary, relevant and cost effective by ICT Unit in consultation with requisitioning department.

To the greatest extent possible the ICT Unit shall ensure that ICT cost and ICT footprint is kept to a minimum. End users shall be allocated the required computing equipment for official use only. Approval for additional equipment must be approved by a relevant ICT committee.

The ICT unit shall make reference to minimum hardware specifications provided in the Directorate of e-Government Standards document.

The ICT unit shall endeavour to consult and share information with other agencies for continuous improvement in the ICT equipment specification process.

Procurement Specification Principles

When developing specifications, the following equipment considerations shall be made;

a) Total lifecycle: These specifications are meant to ensure that equipment acquired have useful life of not less than five years.

`

b) Functionality: This intends to guarantee that operational requirements intended to be performed by ICT equipment can be achieved effectively and efficiently with the equipment specified.
c) Security: This addresses the need to protect system data and equipment, and the operational environment from loss or compromise.
d) Interoperability: This seeks to facilitate the exchange of information between potentially heterogeneous systems through conformance to open standards.
e) Compatibility: This addresses the ability of ICT equipment components to effectively and efficiently work together in an integrated system.
f) Scalability: This is intended to ensure that the acceptable ICT components enhance the ability of the equipment to support future growth and increased throughput.
g) Availability: This seeks to maintain operational readiness through robust and/or redundant (e.g. fault tolerance) equipment.
h) Accessibility: This addresses operational readiness that includes the ability of users and operators to access the equipment in a timely fashion, to perform its intended functions.
i) Long-term support: This addresses the availability of vendor and/or internal support, including parts and labour.
j) Upgradability: ICT component installations that need updates shall be updated according to the latest official versions available.

The ICT unit shall use requisition and acceptance forms to ensure that requests for procurement of ICT equipment are approved by the respective Heads of Department.

Evaluation

Technical evaluations led by ICT Unit shall ensure that the equipment is fit for the purpose intended and that it meets the required specifications.

The Head of ICT Unit shall ensure that warranty agreements and guarantees are provided and also oversee administration of the same. The minimum warranty for all ICT equipment shall be one year, and three years for servers. All warranties shall be in writing.

The ICT Unit or a member appointed by the Head of the unit shall be involved in the technical evaluation and inspection processes.

Inspection

The ICT Unit shall develop guidelines to aid inspection process. Where no ICT personnel are available, the responsible officers on the ground will be guided by the inspection guidelines while ICT Unit shall maintain oversight.

Upon delivery of the equipment, the ICT Unit shall inspect and ascertain that they meet or exceed the specifications as requisitioned.

The ICT head or an ICT officer appointed by the head shall work in conjunction with the relevant ministerial inspection and acceptance committee to validate the receipt of all ICT equipment procured or donated to the Ministry.

All acquisitions and donations shall be required to meet the minimum specifications.

Inventory

All equipment received through purchase or donation by the MoH shall remain the property of ministry and must be tagged appropriately.

The ICT and the procurement units shall maintain manage and take custody of the inventory of all ICT equipment for the ministry.

All equipment and assets whether new, transferred and/or write-off shall be recorded by the ICT Unit for audit and other asset managerial purposes.

The inventory of ICT assets shall indicate product details (product number, serial number, part number, etc.), tracking information, maintenance schedules and warranty information.

Officers exiting the Ministry shall be required to surrender all ICT equipment in their custody to the ICT unit.

Installation and Operation of ICT Equipment

Installation of ICT equipment includes but is not limited to equipment upgrades, part replacements, assembly, and part transfers, among others.

General Installation and Operation Guidelines

a) The hardware installation shall have sufficient capacity to serve the Ministry
b) The ICT equipment shall work as designed
c) The hardware shall work well and without failure
d) Before installation, the equipment must be tested to ensure they work as required.
e) The equipment shall be used for the intended purpose.
f) Associated licensing for the equipment need to be validated.
g) Only qualified personnel shall be allowed to install the ICT equipment
h) The installation of ICT equipment shall adhere to the OEM instructions.
i) Only trained and qualified personnel will be allowed to operate the ICT equipment
j) ICT equipment shall be operated within recommended environmental conditions of temperature, humidity, etc.
k) Access and maintenance of equipment shall only be carried by authorised and accredited personnel.

Administration

The ICT Unit will be responsible for administering ICT infrastructure, including ICT equipment.

Specific authority shall be obtained from the relevant section head before installation and operation on ICT equipment can be undertaken.

Installations that will affect mission critical equipment shall require prior notifications to equipment administrators and users of the anticipated downtime.

Where equipment has to be moved, a document to track movements of hardware shall be used.

`

End-users are prohibited from carrying out any installation, maintenance or upgrade of whatever nature.

Change management guidelines

Change management of ICT equipment shall be guided by the following considerations:

a) Define nature of installation or operation
b) Reason for the change
c) Specification of client services affected
d) Any prerequisites and fall back plan
e) Who is involved in the installation/operation
f) Required time and resources for the installation
g) Details of the change instituted

Prohibition

ICT equipment that does not meet industry and safety standards is prohibited from being deployed.

ICT Equipment Assessment and Audits

The ICT Unit will periodically conduct assessment/audit of ministry ICT equipment to ensure compliance with performance standards and requirements, and ensure equipment component parts are as indicated in the inventory.

Maintenance

ICT equipment maintenance may be done in-house by ICT Units where a maintenance function shall be established. The unit shall develop a schedule of maintenance for equipment as well as an equipment upgrading plan.

Sub-contracting for maintenance shall be through appropriate justification and approval by the Accounting Officers in consultation with the ICT Unit. Due diligence shall be undertaken in engaging and retaining such contractors.

The Head of ICT Unit shall prepare an annual maintenance report and forward it to the Accounting Officer.

ICT Units shall undertake surveys to identify obsolete equipment for the purposes of disposal. Where such equipment contains data, that data shall be permanently erased using suitable mechanisms

ICT Unit shall electronically track the physical locations and status of all equipment where possible.

The ICT unit shall draw up a maintenance schedule of all equipment under its custody. The schedule shall specify the frequency levels and type of maintenance for each type of equipment.

In case of mission-critical equipment, users shall be notified of the maintenance in advance.

The ICT unit shall ensure that the vendor’s SLAs terms are made to the satisfaction of MOH.

`

ICT equipment maintenance shall consider routine/preventive, upgrade, and repair maintenanceas may be required.

Decommissioning and Disposal Guidelines

Decommissioning is the formal termination of equipment and its removal from the IS operating environment. The ICT unit may decommission equipment that is no longer needed on it's IS.

Equipment may be decommissioned if it meets one or more of the following criteria:

a) Redundant equipment
b) Change in IS architecture
c) Technologically obsolete equipment Insufficient capacity to handle application and/or user requirements
d) Where upgradability options have been exhausted
e) Where equipment has become unsafe

Decommissioning of equipment will be undertaken through committee. Candidate equipment for decommissioning determined to be still useful and still meets the required safety standards may be reassigned to lesser demanding tasks or appropriate environment.

Decommissioned equipment that is no longer required shall be treated as candidate items for disposal.

MoH may dispose of equipment that it deems no longer useful.

Identification of the equipment for disposal shall be based on the following criteria:

a) Damaged beyond repair
b) It cannot be upgraded
c) If the repair cost is higher than the cost of buying a new one (cost will either exceed or is considerably close to the cost of acquiring a new replacement)
d) If the parts and/or consumables are not available
e) End of life and no longer supported by the OEM

Departments wishing to dispose of ICT equipment should seek advice from the ICT unit.

Disposal Mechanisms

When equipment is identified for disposal, all application software and data should be backed up and permanently erased from the equipment in accordance with the relevant regulations or guidelines. The inventory tags shall also be removed and destroyed while updating the inventory system.

Equipment identified for disposal shall be handed over to the ministerial committee on disposal to be disposed of in accordance with the relevant disposal regulations.

ICT equipment identified for disposal but deemed to be still usable may be transferred to other agencies and installed for low-end non-critical use where appropriate. Adherence to the statutes and regulations on disposal must always be observed.

ICT equipment for disposal shall be tagged with the standard Government labelling conventions and appropriately physically secured.

The ICT unit shall electronically keep an inventory of all the ICT equipment that has been disposed of.

Equipment may be disposed of by Cannibalizing ICT equipment that cannot be used in whole. Such equipment may be cannibalized for those components. Proper records shall be kept to indicate where such components are used or stored.

The ICT Unit may recommend the following alternative methods for disposal to the Ministry:

a) Donation: The Ministry shall upon authority from the Accounting Officer donate identified equipment and components, to deserving Government institutions.
b) Trashing: ICT equipment that cannot be sold and have no useful components, and are not worth donating, shall be trashed. Such equipment shall be forwarded to licensed e-waste handlers through the right disposal channels.

The Head of ICT unit shall give advice before any ICT equipment is disposed of by the MoH.

VIRTUALISATION AND THIN CLIENT, AND CLOUD COMPUTING

Virtualization and cloud computing technologies can help enterprises significantly reduce their desktop/server footprint. By leveraging thin client provisioning, linked clones and application streaming, the user desktop can be delivered without requiring high-end PC hardware, expensive software licenses, and high capacity network connections. These technologies can greatly enhance utilization of IT service, reduce downtime, cut desktop costs, eliminate hardware and platform duplications, and foster work from anywhere on any device for departments.

The Ministry of Health Virtualization and Thin Client Computing standards and guidelines seeks to encourage adoption of virtualization, thin clients and cloud computing technologies in its ICT programs to achieve IT efficiency.

Server Virtualization

Virtualizing servers can significantly reduce the number of physical servers needed to compute without compromising on service availability. Typical consolidation of x86 servers commonly results in server savings in the ratio of 18:1 if conservatively done. A complete consolidation strategy for data center integrates unified communications, virtualized desktops and servers, and automated storage. The Ministry of Health shall use Server Virtualization and Consolidation as an avenue to;

- *Improve standardization:*
  Standards are easier to enforce across fewer servers. For example, with fewer servers to monitor and manage, the Ministry easily ensures that they are running the same version of software, including service packs and patches, which benefit the Ministry in making management of the servers more consistent and efficient.

- *Improve utilization:*
  Improvements to server scalability—that is a system's ability to easily accommodate additional load, as well as the ability to run applications side by side and manage their resource allocation—can lead to better server utilization. Having fewer servers also creates opportunity for fewer software licenses, or the opportunity to ensure better utilization of software licenses.

- *Improve security:*
  Fewer servers present a smaller attack surface and create an environment that is easier to monitor for security problems and patch in the event of vulnerabilities.

`

- *Improve management:*
  Fewer servers combined with the other improvements of consolidation, such as reducing the number of locations where servers are installed, allow the administrators to do a better job managing them, such as keeping them up-to-date with patches.

- *Improved business intelligence:*
  Consolidating data on fewer servers creates opportunities to mine it for information that could not be as easily accessed and analyzed were it stored in multiple, disparate databases.

- *Improved facilities utilization:*
  Centralizing and reducing the numbers of servers reduces the number of computer or server rooms that require specialized power, conditioning, and physical security.

Managed Desktops and Virtual Desktops

Desktop computing can be converted from device-centric to user-centric computing model. This ensures that a user's computing environment follows them around. Managed desktop decouples OS, applications and user data from the underlying PC hardware. A virtual platform can deliver entire desktop. Centralized and automated management of the desktop infrastructure is then possible.

Government desktop environment is predominantly standard x86 running Microsoft Windows operating system. These desktops can be virtualized to reduce environmental and security risks to ensure government can still operate at desktop level in the event of a disaster. Virtual desktops can be integrated with a cloud computing solution, server and storage virtualization. Virtual desktops greatly reduce environmental and support costs. Virtual desktop devices may be swapped out when they malfunction while baseline OS images and pre-packaged applications are easily deployed.

The desktop virtualization guidelines recommend the use of virtualization of user desktop environment where possible.

Thin Clients

As opposed to standard desktops, thin clients are small and agile. By using a connection, thin clients establish user session to the Virtual Desktop Infrastructure (VDI) servers that provide the virtual desktop for that user. VDI sessions are bound to user ID.

Thin client computing delivers benefits in patch management, centralized management, rapid deployment, set and forget virtual centers, and desktop OPEx among others. This guideline recommends the use of thin clients in large desktop deployment scenarios such as Ministry customer relationship centers, where the need for a rich client is not mandatory.

Cloud Computing with Virtualization

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned on demand, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the best of both worlds, providing solid support for core business functions along with the capacity to develop new and innovative services.

Cloud computing Models

Cloud computing models vary: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Management of cloud computing service levels is via the surrounding management layer.

- **Infrastructure as a Service (IaaS).** The IaaS layer offers storage and compute resources that developers and IT organizations can use to deliver business solutions.
- **Platform as a Service (PaaS).** The PaaS layer offers black-box services with which developers can build applications on top of the compute infrastructure. This might include developer tools that are offered as a service to build services, or data access and database services, or billing services.
- **Software as a Service (SaaS).** In the SaaS layer, the service provider hosts the software so you don't need to install it, manage it, or buy hardware for it. All you have to do is connect and use it. SaaS Examples include customer relationship management as a service.

Cloud computing deployments

Cloud computing happens on a public cloud, private cloud, or hybrid cloud. Governance and security are crucial to computing on the cloud, whether the cloud is in your organization's firewall or not.

- **Public clouds** are virtualized data centers outside of your organization's firewall. Generally, a service provider makes resources available to the organization, on demand, over the public Internet.

- **Private clouds** are virtualized cloud data centers inside your organization's firewall. It may also be a private space dedicated to your organization within a cloud provider's data center.

- **Hybrid clouds** combine aspects of both public and private clouds.

Cloud security guidelines

The Ministry of Health shall adopt the following security principles which represent general best practice implementations for cloud security. However they are not intended to be interpreted as a guarantee of success.

- Implement and maintain a security process.
- Build and maintain a secure cloud infrastructure.
- Ensure confidential data protection.
- Implement strong access and identity management.
- Establish application and environment provisioning.
- Implement governance and audit management processes.
- Implement a vulnerability and intrusion management program.
- Maintain environment testing and validation.

Where applicable the Ministry of Health shall endeavor to move data and applications to the cloud to realize flexibility and efficiency in IT service delivery, as well as reduce cost of infrastructure ownership.

Government offices require applications for office collaboration, email, core database, internet and general office productivity. These applications can easily be standardized and managed centrally as a virtual application layer, typically referred to as Software as a Service (SaaS). A robust virtualization platform provides high levels of availability and reliability. When coupled with private or public cloud service IT service responsiveness is assured. Such an IT setup can drive down typical data centre, power and cooling costs by more than 60 per cent.

The Ministry of Health will promote new technologies in virtualization and cloud computing in order to gain efficiency in IT service and realize higher levels in service availability and reliability.

SOFTWARE STANDARDS AND GUIDELINES

Information System is an integrated set of components i.e. software, hardware, and human resource for collecting, storing and processing data and for delivering information, knowledge and digital products in an organization. Software is a set of programs, procedures and algorithms that instruct the computer how to carry out specified functions. The standard provides and prescribes best practices for software development, acquisition, support and maintenance by MoH. These best practices have been recognized to significantly contribute to the successful acquisition, deployment and utilization of information systems.

Software guidelines and standards aims to assure software quality, ensure software internal usability, and help evaluate the software product. Their application by the MOH aims at achieving the following objectives:

i. Ensure data/ information sharing across MOH;

ii. Enhance user satisfaction;

iii. Ensure compatibility;

iv. Enhance unified support and management;

v. Ensure cost effectiveness ;

vi. Provide a platform to support a unified HIS

vii. Improve staff productivity;

viii. Ensure coherence in systems upgrade management.

In addition, when deploying software the MoH shall ensure conformity to WHO Health Informatics Standards and software international standards including but not limited to:

i. ISO 9126- 1 on Software product quality

ii. ISO/IEC 9126-2 on External usability metrics

iii. ISO/IEC 9126-3 on Internal usability metrics

iv. ISO/IEC 9126-4 on Quality in use Metrics

v. ISO 9241-11 on Guidance on usability

vi. ISO 14598 – 1 on Software product evaluation.

vii. ISO 27799 – Information security management in health using ISO/IES 27002

The guidelines shall publish acceptable standards for software products bought off-the shelf, Free and Open Source Software (FOSS), software developed internally or developed by contracted third parties. For the purpose of this guideline, software is classified in three broad categories based on its purpose, functionalities, type, or area of application:

1. Application software.
2. System software.
3. Application Development software.

ACQUISITION OF APPLICATION SOFTWARE

Application Software

Application software refers to computer software designed to perform a specific set of tasks.

Acquisition of application software, unlike other types of software shall require an elaborate approach due to the nature of it specialization. Since applications shall be acquired for a diverse business processes and support services, the procedures guiding this acquisition shall be determined by the nature of the application as well as availability in the market of off-the-shelf programs that address the specific business requirements. In all application software acquisition procedures, a technical committee comprising of business, key stakeholders and ICT subject experts should be set up. In addition, application of a standard software development methodology and project management guidelines shall be enforced.

Acquisition of application software shall therefore fall under the three broad procedures:

1.1.1 In-house Development:

All In-house development of business software shall be coordinated by the ICT Unit. The software development process will adopt a project management approach. The ICT Unit will constitute a development team consisting of various specializations as may be required in specific software development task. These shall include software developers with expertise in target development platform, business/systems analysts, business/systems designers, database experts, network and communication, security specialists, system testers among other skills that may be required in different project.

1.1.2 Outsourced Development:

For sophisticated system development initiatives that require skills and knowledge not available within MOH, an external developer may be contracted to deliver the business application. In this case, the implementing unit/ Department within MOH in collaboration with ICT Unit shall adopt a project and constitute a technical team consisting experts in the business and technical process, business/systems analyst and the relevant ICT skills. The technical team shall:

a) Develop a concept paper and seek approval from the ICT governance committee
b) Develop a Request for Proposal/Terms of Reference including well-articulated and comprehensive business and functional requirements that shall inform a contractor to enable them in the submission of proposal that delivers a turn-key business solution.
c) Evaluation of both the technical and functional requirements to ensure that they are clearly aligned to the needs of the ministry.
d) Ensure that the contracted firm delivers source codes, implementation manuals, end user manuals and all other necessary documentations.

e) Manage the entire process using the acceptable project management methodology

f) Establish and ensure conformance to the Service Level Agreement

1.1.3 Commercial off-the Shelf:

A project technical team in some cases having developed the business and functional requirements in software development process may seek to acquire a solution that is readily available in the market. Examples of such solutions include modules of ERP software. In this case, the implementing agency within MOH in collaboration with ICT Unit shall constitute a technical team consisting experts in the business process, business/systems analyst and the relevant ICT skills. The technical team shall:

i. Develop a concept paper and seek approval from the ICT governance committee

ii. Develop a detailed specification of the system that comprehensively meets the business and functional requirements of the client.

iii. Review existing deployment of such systems for the purposes of benchmarking.

iv. Manage the entire process using the acceptable project management methodology

v. Ensure proper knowledge transfer to the client for sustainability of the system

vi. Ensure that the contracted firm delivers implementation manuals technical manuals, end user manuals, licenses and all other necessary documentations.

vii. Ensure there is a contract document on post implementation that includes Service Level Agreement, warranties, Support and Maintenance for a minimum of two years

`

SYSTEM SOFTWARE SPECIFICATION

Systems Software

System software refers to computer programs used to start and run computer systems and networks, including but not limited to Operating Systems.

MoH shall endeavor to upgrade, to the minimum requirements, all software that fall below the recommended standards. MOHs shall ensure that:

i. Licenses for commercial operating system are provided upon acquisition, duly registered and subsequently renewed as per the requirements of the copyrights;

ii. The latest stable version is purchased in each case;

iii. Vendor Support is provided;

iv. The software is regularly updated with the latest patches.

v. Shall ensure that only licensed system software is used

ICT units shall keep an inventory of all operating system software installed and closely monitor and evaluate to ensure licensing and copyright agreements are maintained. The head of the units shall take custody of all Operating System software installation materials, including manuals and related materials where supplied. They shall also ensure that where possible, back-ups are carried out before any reinstallation or upgrade of an operating system. The units shall organize training for users on any new client operating system software.

`

Application Development Software

Application development tools are used to translate and combine computer program source code and libraries into executable programs i.e. compilers and linkers.

MOH shall ensure that ICT officers responsible for development of software are adequately trained on all application software acquired.

MOHs shall take into consideration the following when acquiring application development software:

a) Type of application to be developed; Desktop application, Web based application or server application and mobile application.

b) Operating System platform the software to run on.

c) Integration with the existing development tools.

d) Database to be used by the application.

e) Compatibility with existing and future hardware and software platforms.

f) Assistance in enforcement of coding Standards

g) That has community support base

Software Acquisition

Customized Commercial Software (COTS)

Below are the minimum requirements that must be considered in the acquisition of COTS:

- **Total lifecycle cost**. This cost includes initial costs such as purchase, installation and training, plus the on-going cost of maintenance and support.
- **Maintainability**. This criterion addresses the ability to administer and perform corrective, adaptive or perfective maintenance on the COTS product within defined tolerance for cost and service, using vendor and/or internal support. This criterion

`

includes minimal operational disruptions and downtime, the ability to tune the software to improve efficiency and effectiveness and the cost and effort to upgrade to improved versions of the software product.

- I**nteroperability**. This criterion seeks to minimize the additional support required to integrate the COTS product as a functioning component in the MOH IT portfolio. As an example, the exchange of information between potentially heterogeneous systems can be facilitated through open standards or non-proprietary protocols (e.g., TCP/IP). Interoperability should include flexibility in supporting changes over time and among multiple state agencies and systems. Interoperability standards affecting more than one Agency shall be mutually determined and consistent with all higher-level (e.g., Statewide) standards.
- **Portability**. This criterion addresses the ability of an existing software component to move from one physical or logical position in the IT infrastructure with minimum impact on cost and service.
- **Scalability**. This criterion ensures that acceptable COTS software products enhance the ability of the system to support future growth and increased throughput necessary to meet e-Government goals. This objective is achieved through excess capacity or the flexibility to easily modify and/or enhance the system as needed (e.g., application performance or transaction process speed, forward and backward compatibility, modularity, etc.).
- **Availability/Accessibility**. This criterion seeks to maintain a system's operational readiness and required level of service without disruption from software failure. This is achieved through robust and/or redundant (e.g., fault tolerant) software. Operational readiness will include the ability of users and operators to access the system, in a timely fashion, to perform its intended functions.
- **Reusability**. This criterion addresses the ability to make repeated use of the COTS software product for additional requirements with minimum additional cost.

- **Functionality/performance.** This criterion seeks to guarantee that the MOH Operational requirements, especially its mission critical requirements, intended to be performed by IT systems, can be achieved effectively and efficiently with the specified COTS software. It includes the properties of efficient software/hardware integration that affects the ability of the overall system to perform adequately to meet operational requirements.

- **Security**. This criterion addresses the need to protect system data and the operational environment from loss or compromise. It includes the ability of the COTS software to prevent and contain malicious as well as non-malicious security breaches.

- **Other Specific Criteria**. Other criteria are explicitly used for specifying the acceptable set of COTS software products. For example, vendor viability, licensing restrictions, potential product market share, customer recommendations, and product volatility (e.g., frequency of upgrades and potential obsolescence) may be important.

Open Source Software

Open software enables access to the source code written in the programming language in which the special-purpose software is written, which allows the expert users to read, modify and adapt the open source software to current purposes. Open software is at the same time computer software whose source code may be freely redistributed and modified

In acquiring Open Source Software the ICT unit shall:

1. Develop a detailed technical OSS specification that meet the client needs
2. Identify the Open Source Software that could provide solution for the target information system

`

3. Solicit and evaluate various OSS offers in the market.

4. Consider licensing that come with OSS

Application software

Application software is computer software designed to help the user to perform singular or multiple related specific tasks. Examples include enterprise software, accounting software, , graphics software, office productivity software, utility software, security software, web development and management software, database software, communication software, network management software and media players.

ICT Unit shall ensure that:

- The latest stable versions of application software are installed in user computers and that security and software updates are made as soon as they are released. Where a previous version is to be used adequate justifications are to be provided.

- Users are adequately trained on the use of any application software purchased.

- All application software acquired are adequately supported and maintained by the vendor.

Software Development

MOH shall encourage the development of custom software applications where necessary. Custom software or bespoke software is software that is specially developed for the client. It contrasts with the use of software packages developed for the mass market, commonly referred to as commercial off-the-shelf (COTS) software, or free software. Custom software can be developed by MOH in-house software development group, or be commissioned from a software house or independent software developer.

`

Custom software can accommodate an MOH's particular preferences and expectations. They may also be designed stage by stage to take into account all issues including those not mentioned in the specifications.

It is recommended that an optimal system development methodology such as software development lifecycle be adopted in order to obtain a useful system. In addition, a software development process must adhere to project management principles as they may be defined in the Project Management Guidelines.

System Development Process

The System Development process encompasses all activities involved in the development of application system. Such activities include requirements gathering, analysis, design, construction, testing, implementation, and maintenance.

The MOH shall use SDLC in developing applications in a well-defined, disciplined, and standard approach. It provides a methodological approach and a platform for managing, directing, monitoring and controlling the process of application or software building, including description of the process and deliverables.

To obtain good results from the SDLC methodology, its stages must be strictly followed:

- Requirements gathering and system analysis
- System Design
- Development and Implementation
- System Testing
- Operations and maintenance
- Post implementation monitoring and evaluation

`

MOH shall adopt the following methodology which is derived from SDLC and outlines the specific activities in each phase as well as the outputs and deliverables of the stage.

Software Development Lifecycle

It is imperative that all software development projects have a comprehensive Project Charter precedent to project initiation. In addition, the processes must adopt a documentation standard including: Context Diagram (CD), Entity Relationships Diagrams (ERD), Data Flow Diagrams (DFD) and Process Maps as appropriate at every stage.

Procurement

Procurement of software shall be done with consultation and coordination of the ICT Unit which shall be responsible for the preparation and issuance of all technical specifications for the software, as well as ensuring that the guidelines stipulated herein are adhered to. MOH shall use requisition and acceptance forms to ensure that requests for procurement of software are validated by the respective Heads of Department. MOH shall also ensure that requirements are clearly defined and documented when procuring enterprise software. Where possible, MOH shall endeavor to use enterprise version of software, depending on the requirements of the user.

MOH shall make sure that there is no already existing software application within MOH that provides equivalent functions and that can be replicated in the organization before procuring any software to avoid duplication.

All ICT software procured or donated to MOH shall be received by the ICT Unit which shall ensure proper custody and issuance. All donations shall be required to meet the minimum specifications. Furthermore, all software assets (new, transferred and/or written off) shall be recorded by the ICT Unit for audit and other managerial purposes.

MOH shall endeavour to procure and use the latest version of software. Where a previous version of software is to be used, the user shall be required to give justifications.

Technical evaluation shall be undertaken to ensure that the software is fit for the purpose it is being acquired for and that it meets the provided specifications. Upon delivery of the software, ICT Unit shall inspect and ascertain that they meet the laid down specifications. The ICT Unit shall ensure that technical evaluation and inspection reports are prepared respectively.

The ICT Unit shall ensure that an agreement is in place to warrant software support and replacement when required, and that such agreements acquired are enforced. When the software is procured, related licenses should be adhered to, and that the vendor should guarantee subsequent licensing arrangements.

The procurement procedures as stipulated in the public procurement and disposal act 2005 shall be followed.

Maintenance

ICT Units shall keep an inventory of all software in the MOH, and give quarterly reports on status of utilization, support, adaptability and licensing status.

ICT Unit shall also determine which software have expired licenses for the purposes of renewal, upgrade or disposal. Where such systems have proprietary data, that data shall be extracted using suitable mechanisms.

Software media and administration documentation, whether hardcopy or electronic, shall be securely stored in a central repository and copies may be created for backup and disaster recovery purposes as permitted by the license terms and conditions. Software media shall be tagged with the standard government labeling conventions and appropriately physically secured.

Software maintenance shall be done in-house by ICT Units who shall develop a maintenance schedule on upgrading and debugging. Sub-contracting for software maintenance shall be through appropriate justification and approval by the ICT governance

`

committee. Due diligence shall be undertaken in retaining such contractors. The ICT Unit shall prepare an annual maintenance report and forward it to the ICT governance committee.

Disposal

The ICT Unit may justifiably replace software with newer versions or replace no longer required the software for various reasons:

- Replacement by a newer version
- No longer used in the department
- Obsolescence
- All retired software may be destroyed in accordance with manufacturer end-user license agreements and copyright laws. Generally, if the software is to be discarded, media should be damaged to prevent subsequent unauthorized use.
- Upon retirement of computer equipment, all software and data must be removed from computer hard drives to ensure software license compliance, user privacy, and the security of institutional data.
- The ICT Unit on assessment of the software may advice on transfer of software ownership, retirement or redistribution to another location within MOH.

Prohibited Software

Prohibited software are software that can cause malicious damages to MOH systems, networks and data, those that violate other organization's licensing requirements or that which interfere with MOH network throughput.

It is expressly forbidden to possess, distribute, reproduce or use computer programs for reasons such as scanning networks, intercepting information or password capture unless specific authority is obtained or held.

`

Software copyright compliance

1. The MOH will only use a genuine copy of legally acquired software that is configured and used in accordance with the license terms and conditions as set out by the copyright holder.

2. The making or use of unauthorized or illegal software copies is prohibited in all MOH. Where possible, controls will be in place within the MOH to prevent the making or use of unauthorized or illegal software copies. These controls shall include effective measures to verify compliance with acquired software licenses.

Software Audits

MOH shall periodically conduct audit of software in MOH, to ensure that they comply with all software licenses and the software developed meet the required guidelines.

Training and Knowledge Transfer

MOH shall ensure that ICT officers mandated to maintain or support software acquired are adequately trained. Where a maintenance contract is in place, MOH shall ensure that measures are put in place to enforce knowledge transfer to ICT officers by contractors and vendors for continuous support and maintenance of the system once the contract expires.

Software Custody

1. ICT unit shall have custody of all software under a documentation library.
2. ICT unit shall facilitate training on the acquired software.
3. The Ministry staff shall not borrow or lend any software.
4. All software developed in house by the Ministry staff shall become property of the Ministry.

Licenses

1. The Ministry shall comply with all laws regarding intellectual property. This applies to all software licensed or developed by ICT staff at/and for the Ministry.
2. The Ministry shall negotiate for corporate licenses for use by all departments.

3. All purchased/customized software must be accompanied by the required licenses as per specifications.
4. All licenses must be in the name of Department/MOH.
5. All purchased/customized software shall be delivered with documentation
6. All software revision shall be accompanied by documentation.

ACCEPTABLE USE OF ELECTRONIC COMMUNICATION

Electronic communication services are used to support administrative, research and service functions of the Ministry of Health (MOH). Users of these services are expected to act in a professional and courteous manner

All staff should ensure that they only use the officially assigned emails for the purposes of official communication. Sending of spam over all forms of electronic communication is prohibited.

Users should be sensitized on copyright laws and the implications of copying, reproducing or retransmitting materials on the web covered by such laws.

Officers should be encouraged to utilise collaboration facilities on the internet and intranet to enhance the performance of their official duties and responsibilities.

Policies to govern email provision

- Email addresses should be generated from users' legal names and must be unique. Duplicate names are resolved by use of an alternate users name
- The ICT Unit should ensure that email services are available at all times with minimal down times
- There should be departmental/role based email to handle enquiries and other personnel complains to departments or to organization as a whole
- ICT unit should ensure email accounts are backed up periodically
- ICT unit should ensure that the server has updated antivirus and anti-spam guard to prevent circulation of spam mail.
- ICT unit should ensure the email solution being used has the provisions to encrypt and decrypt messages transmitted through it.
- Email group should be constituted with explicit authority of head of department and head of ICT. The groups can be based on departments, division, programs or projects.
- The ICT unit shall to the best means possible guarantee integrity of the email system use.

Policies to govern email use

- New users of email accounts should change their password on the first login attempt
- Users are responsible of the contents (text, audio or images) they send. They should ensure email attachments are not virus infected.
- Any user violating the rights and privileges extended to him/her shall have the account deactivated by the ICT unit
- All emails with confidential and classified information should not be circulated to unauthorised persons or institutions
- Sending offensive, discriminatory remarks or use of inflammatory communication over the network is strictly prohibited.
- Unauthorized access or modification of files, passwords, and data belonging to other users whether internal or external is prohibited
- All emails shall have a disclaimer on each email e.g. "This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secured or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited."
- User Ids and passwords should not be disclosed or shared.
- Impersonation is highly prohibited
- Users need to be aware of unsolicited mail
- Chain mails shall not be circulated

Policies to govern intranet

- Users may have read or write privileges or both. This should be determined and approved by the respective head of department and head of ICT.
- Intranet users and groups should be constituted with explicit authority of head of department and head of ICT. The groups can be based on departments, division, programs or projects.

- Users should not use the intranet rights assigned to them to pursue personal interests and this includes doing private business, advertising, and other commercial purposes which also includes sales of goods and services.
- User Ids and passwords should not be disclosed or shared.
- Any user violating the rights and privileges extended to him/her shall have the account deactivated by the ICT unit

Policies to govern internet

- All internet users in the MOH should use the internet for research and other ethical usage.
- All internet users need to be aware of phishing and corrupted web links that may lead to virus infections or other distractions.
- Pornographic sites and other offensive materials should not be accessed, shared, downloaded or watched in the office.
- The ICT unit shall preserve the right to disconnect or discontinue active usage of the internet.

Consequences of inappropriate use of Electronic Communications

Internet users who violate on the rights and the access privileges granted to them by the ICT unit by way of downloading of unauthorised software and materials on the internet, copying, redistributing, are liable of copyright violation and will be prosecuted by the necessary legal authority

Users who intentionally vandalise or harm or destroy other peoples data or networks and this includes but not limited to the uploading of viruses may be prosecuted and their access privileges withdrawn by the ICT unit

`

IT SECURITY GUIDELINES

Information systems are vulnerable both to physical and virtual attacks as well as potential threats. It is therefore paramount that every organization implements controls and protocols to guard against these threats. These standards will define the guidelines for enforcing system controls and security protocols within the MoH.

MOH shall protect its ICT resources through implementation of sound physical, environmental, and administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and unauthorized access by personnel or external parties.

Physical and Environmental Security

Physical access to a system or network provides opportunity for an intruder to damage, steal, or corrupt computer equipment, software, and information. Procedures should therefore be put in place to ensure that systems and networks are physically secure.

In a networked environment it is critical that each party takes appropriate measures to ensure that its system will not be physically breached, thereby compromising the entire network.

Physical security may be the least expensive to implement. However if not implemented it may result serious damages with higher financial and reputational repercussions to the organization. Even the most expensive and sophisticated computer protection software can be overcome once an intruder obtains physical access to the network or computer systems.

Purpose

This section identifies potential physical threats to facilities, hardware, software, and information. This section also recommends best practices to secure computer systems from physical intrusion.

Physical threats include but are not limited to; Natural disasters and calamities, Accidents, Theft and Vandalism

Scope

This applies to all ICT equipment, software or other facilities that is owned or leased by the MoH. In particular it is necessary to physically secure; Server rooms, Data Centers, Storage Media, Servers, Personal computers (PCs), Network and Network access devices, Mobile or portable computing devices.

Physical Access Controls

Where possible, all information resources (including portable information resources) must reside in a protected environment. Physical and administrative security controls must be implemented at each facility to protect against unauthorized access and to protect the physical integrity of IT service resources at the MoH facilities. Such physical and administrative security controls include the following:

a. Physical access controls.

b. Physical protection of Information Resources.

c. Environmental security.

Establishment of Controlled Areas

Controlled areas must be established within the facility wherever more stringent restrictions on physical access and more tightly controlled physical and environmental security are required to fully protect ICT resources. Typical controlled areas may include the following:

i. Data center, Server Rooms and Computer rooms

ii. Telecommunications rooms.

iii. Wiring closets.

iv. Computer operations areas.

v. Media and documentation storage areas.

vi. Operating system software support areas.

vii. Special authorization terminal areas.

viii. Security officers' controlled areas.

ix. Other designated areas,

Information technology resources that process sensitive or critical information must be located in a controlled area.

Access to Controlled Areas

Access to controlled areas must be managed as follows:

a. Should be restricted to personnel whose duties require access to such facilities and who possess appropriate security clearances.

b. Access to controlled areas must be controlled by either mechanical or automated means.

c. Personnel authorized access to the controlled areas must always use their access control identification badge or device to gain entrance to the controlled area.

d. Tailgating and sharing of access badges is expressly prohibited and should be immediately reported.

e. A record of physical access, both authorized individuals and visitors, must be maintained.

f. Automated mechanisms should be employed where feasible to facilitate the maintenance and review of access records.

g. Unauthorized personnel or visitors must sign a visitor log and be escorted by authorized personnel while in the controlled area.

h. Visitor logs must include at a minimum:

    i. Name and organization of the person visiting,

    ii. Form of identification used for authentication,

    iii. Date of visit, time of entry and departure, purpose of visit

    iv. Name of person and title of the authorizing officer.

    v. Periodic review and security violations or suspicious activities shall be investigated and remedial actions taken.

i. Identification badges must be prominently displayed at all times while within the controlled areas.

Establishment of Access Control Lists

Each controlled area must;

a. Establish an access control list of people who have authorized access.
b. Be updated when new personnel are assigned to the controlled area or when someone leaves.
c. Be reviewed, updated periodically, and posted within the controlled area.

Physical Access Control Measures

Physical access control devices using biometrics, smart cards, tokens, mantraps, or lockable cabinets must be installed to supplement traditional facility locks and keys to limit access.

Additionally, the ICT Inspection Service unit and Facility Management may require physical access to be monitored by surveillance equipment and real time intrusion detection and alarm systems (e.g., CCTV, motion detectors, and other audio or silent alarms) to detect and respond to incidents.

Based on the risks associated with the specific information resource, additional physical access security mechanisms (e.g., locked cabinet or desk, portable device cable lock, and biometric workstation lock) must be implemented for information resources processing sensitive or critical information.

Security personnel are notified immediately of physical security events and follow-up action is taken and documented.

Implementation of Identification Badges

Identification badges must adhere to the following criteria:

i. Persons authorized access to controlled areas must be identified by a picture badge conspicuously displayed on their person.

ii. Persons using a badge not issued to them or making any attempt to alter a badge will be subject to disciplinary and/or criminal action.

iii. Employees must report lost or stolen badges immediately to the issuer of the badge.

iv. The rights and privileges associated with badges reported lost or stolen must be immediately revoked.

v. Temporary badges must be controlled and issued at the discretion of the authorized officer or their designee.

vi. The authorized officer or their designee should perform regular verification of badges and address any irregularities.

vii. In the case of attrition by the staff the authorizing officer should ensure that the badges are returned and / or rights revoked.

Physical Protection of Information Resources

ICT resources must be protected against damage, unauthorized access, and theft, both within and out of the secure environment.

Network Equipment and Servers

Network equipment and servers must be protected against damage, unauthorized access, and theft and housed in a controlled area. Additional protection measures to control physical access to information distribution and transmission including secured wiring closets and protection of cabling with conduit or cable trays should be implemented.

Workstations and Portable Devices

Workstations and portable devices must be protected at all times while in use, storage, and in transit against damage, unauthorized access, and theft. Custodians of these devices will be held accountable for their loss, damage or compromise.

Personal Computing Devices

To protect MoH information from disclosure or compromise, any personal computing devices [e.g., laptops, notebooks, personal digital assistants (PDA), handheld computers, or storage media including universal serial bus (USB) port devices or thumb drives] should not be used on Government facilities without approval from the Head ICT Unit.

Critical Media

Critical media that contains sensitive and crucial data whether electronic or non-electronic must be protected against physical loss or damage, whether within MoH premises or not. Physical and administrative controls must be implemented to ensure that only authorized personnel can access sensitive and critical information. Personnel who have custody of sensitive and critical media are responsible for their safekeeping.

Environmental Security

Environmental security controls must be implemented at all MoH ICT facilities including data centers, computer rooms, and offices to protect ICT resources as described below:

a) Protection against lightning, wind, and building collapse must be implemented.
b) Protection against water damage from water supply lines, sewer systems, and roof leaks must be implemented
c) Temperature and humidity safeguards must be implemented to monitor and maintain acceptable levels.
d) Mitigation against flooding, earthquakes or other natural disasters must be implemented (e.g., drains are installed below the computer room floor).
e) Protection against Fire:
    i. Fire detection and suppression equipment (e.g., smoke and heat detectors, handheld fire extinguishers, fixed fire hoses, and sprinkler systems) must be implemented
    ii. Fire detection and suppression equipment must automatically notify the organization and emergency responders.
f) Additional power (electricity) safeguards:
    i. A short-term and long-term alternate power supply must be implemented to ensure continuity in the event of a power interruption.
    ii. Emergency lighting systems must be implemented to illuminate emergency exits and evacuation routes in the event of a power outage or disruption.
    iii. Surge protection must be implemented for critical ICT Equipment.
    iv. Redundant power feeds and redundant communications paths must be implemented for critical information technology sites.

Where environmental hazards are eminent or in the process of occurring in areas of concentrated information resources the following measures shall be undertaken by facility management where possible;

`

a. Initiate remote or automatic shutdown of power to facility
b. Isolate the controlled area
c. Invoke the facilities emergency procedure
d. Invoke data center emergency procedure.

Each facility shall develop its own environmental emergency procedures.

Account and Password Management

Access to information resources is managed through the use of multiple types of accounts, including; User, Privileged, Service, Maintenance and Guest account.

Ownership for privileged, shared, and maintenance logon IDs must be documented and administered in a secured manner.

Account Management

Accounts must be established in a manner that ensures access is granted based on clearances, need to know, separation of duties, and least privilege basis.

The following are the prescribed principles to guide the accounts management:

User Accounts

User accounts should provide application/platform users with a minimum level of information resources and application functionality needed to perform their duties;

a) Least privilege – user account should not carry special privileges above those required to perform the user's business function,
b) Access to account shall be restricted to a specific purpose (e.g., an auditor account),
c) Access to application shall be via approved front-end interface (e.g., web client accounts) that confer defined account privileges and roles,
d) Platform user accounts (i.e., database and operating system) shall have limited access rights.

Privileged Accounts

Privileged accounts, such as administrator or maintenance accounts at application or platform-level (i.e., database and operating system) accounts shall have higher levels of rights such as account creation/update/deletion, full application/platform functionality, or a subset of rights that have been designated as privileged.

Privileged accounts management shall be guided by following principles;

a) Assignment of privileged accounts must be restricted to unique individual whose duties require additional privileges and whose job functions require such account,
b) Individuals must not use their privileged accounts to perform non privileged functions.

`

c) Application accounts must not have the capability to run as “root,” and
d) An audit trail must be maintained on all privileged account usage.

Service Accounts

Service accounts shall be assigned to an information resource (e.g., server, application) or other automated process/service (not an individual) used to process data and/or identifies actions or requests.

Service accounts management shall be guided by following principles;

a) must be placed under management control,
b) must be created with the minimum access rights and privileges required to perform the necessary business function, and
c) Must not be allowed root or administrative privileges.

Non-expiring Service Accounts

The rationale for these accounts is to prevent service interruptions due to a locked account. The following compensating controls must be implemented with service accounts:

a) Account must be documented.
b) No privileged access shall be allowed; specific ACL's must be applied under the concept of 'least privilege'. Use of root, system administration, non-cancel, etc. privileges is prohibited.
c) Account must not have the rights to modify or delete system (e.g., syslog or Windows System Event) or security log files.
d) Restrict account's usage to a specific host.
e) Direct login using the service account, whether from a console or remote session, is prohibited and must be disabled.
f) Rights and privileges of account must be reviewed and validated on annual basis.
g) Non-expiring password must meet password length and complexity, and be encrypted in storage and in transit.

Maintenance Accounts

Vendor default accounts shipped and/or pre-installed on a vendor product must be removed or disabled. Vendor maintenance accounts must be enabled only when needed and controlled by a responsible government information technology service entity.

Guest Accounts

Guest accounts shall not be allowed access to MOH information technology network information resources. Guest accounts incorporated into any software or established through any other means must be disabled.

`

Establishing Accounts

To establish an account, personnel must request an account from their manager or supervisor. A database of all users or potential users of a system should be kept preferably in a directory.

Documenting Account Information

The account information for each user account, or database, must contain the following information: logon ID, group memberships, access control privileges, authentication information, and security-relevant roles.

Any security-related attributes that are maintained must be stored securely to protect their confidentiality and integrity.

Configuring Account Time-Outs

Accounts must be configured to automatically log the workstation off the network or disable the session after a predetermined period of inactivity and enforce re-authentication.

The MOH information technology default standard period of inactivity is a maximum of 15 minutes.

Any deviation from this must be documented and approved by the Head of ICT or their designee.

Suspension of User Accounts

Suspension of user accounts shall be guided by the following principles;

a) Accounts of MOH employees/MOH Information Systems users who leave must be disabled immediately,
b) Accounts shall be suspended when the owners are on leave/vacation. However this may be reviewed if the account holders have written permission from Head ICT to access MOH system while on leave/vacation.

Maintenance of Vendor Accounts

Vendor accounts must be strictly managed, enabled only when needed by the vendor, and monitored while being used.

Handling Compromised Accounts

Information resources must provide automated mechanisms to support identifying and handling information security incidents. All personnel who suspect an account has been compromised must immediately notify management and follow the incident reporting process.

Identification

Identification is the process of associating a person or information resource with a unique enterprise-wide identifier (e.g., a user logon ID). A logon ID is used in conjunction with other security services, such as authentication measures, to track activities and hold users accountable for their actions.

Users shall be responsible for all actions performed on MOH information technology resources under their logon ID.

Security Identification Requirements

Information resources must comply with security requirements including, but not limited to, the following:

a) The information resource must, at a minimum, use logon IDs as the primary means of identification.
b) The information resource must have the capability to automatically disable a logon ID that has not been used for an administrator-configurable period of time.
c) The information resource must not allow an administrator to create, intentionally or inadvertently, a logon ID that already exists.
d) A logon ID must not exist without associated authentication information.
e) The information resource must not provide any process to bypass the authentication information for any logon ID.
f) The information resource must have the capability of associating each internal process with the logon ID of the user who initiated the process. Processes that are not initiated by a user, such as print spoolers, database management servers and any spawned sub-processes, must be associated with an identifier code, such as "system ownership."

Issuing Logon IDs

Logon IDs are unique groups of letters, numbers, or symbols assigned to a specific person or information resource.

All personnel using MOH information technology resources shall be issued a logon ID according to a prescribed authorization process.

No two users may be assigned the same logon ID.

Protecting Logon IDs

Logon IDs must be protected in accordance with the following principles;

a) Personnel must not share their logon IDs or permit others to use them to access government IT resources, and
b) Logon IDs must not be embedded in application code or batch files or stored in application files or tables unless approved compensating security controls are implemented.

Suspending Logon IDs

Suspending logon IDs shall be guided by;

`

a) Lock out an ID for a period of at least 15 minutes after six unsuccessful attempts to log on to an information resource,
b) An ID shall remain locked out upon expiration of the lock-out period until the user contacts the Help Desk and follows the defined procedure for account reinstatement, and
c) IDs not used within the last 180 days must be disabled.

Handling of Failed Logon Attempts

Failed logon attempts must be recorded for audit trail and incident reporting purposes.

Notification to the user of a failed logon attempt will reflect only that the logon failed. The reason for the failed logon attempt and information previously entered, including the disguised or clear password, must not be returned to the user.

Terminating Logon IDs

Logon IDs not used in the last year must be deleted.

Authentication

Authentication is the process of verifying the claimed identity of an individual, workstation, or originator. Authentication is achieved when the user provides the correct password, personal identification number (PIN), or other authenticator associated with that identifier.

All MOH Personnel must be required to identify and authenticate to the information resource before being allowed to perform any other actions.

Means of authentication, or authenticators, may include the following:

a. Passwords

b. Personal identification numbers.

c. Shared secrets.

d. Digital certificates and signatures.

e. Smart cards and tokens.

f. Biometrics.

g. CAPTCHA.

Passwords Management

Passwords are unique strings of characters that personnel or information resources provide in conjunction with a logon ID to gain access to an information resource.

As the first line of defense for the protection of MOH IT resources, passwords must be treated as sensitive information and must not be disclosed.

Password Selection Requirements

Password requirements must comply with the following:

a) For privileged users (users with administrative rights), passwords must consist of at least eight characters and contain at least one character from three of the four following types of characters: English uppercase letters (A–Z), English lowercase letters (a-z), Westernized Arabic numerals (0–9), and non-alphanumeric characters (i.e., special characters such as &, #, and $). It is recommended that system administrators use two-factor authentication. For other non-privileged users, passwords must be of at least eight characters and at least one non-alphanumeric character.
b) For all users, passwords must not contain the user's name or any part of the user's full name.
c) Passwords must not be repeated (reused).

Password Selection

The following password recommendations are prudent security practices intended to enhance the password complexity and protect the password from attempted password cracking:

a) Do not use family member names or other information easily discovered about the user (e.g., license plate number, phone number, birth date, and street name).
b) Do not use commonly used words such as words that appear in the dictionary.
c) Do not use all the same characters or digits or other commonly used or easily guessed formats.
d) Use longer password conventions whenever possible

Initial Passwords

Passwords must always be delivered in a secure manner. The initial password for users must be sent via protected electronic delivery system or personal delivery to the user.

For all accounts, the initial password must be set to a temporary password, and the user must be required to change the password at first logon.

Caution must be taken not to standardize on generic or global passwords when issuing new accounts or when resetting forgotten passwords.

`

Password Suspension

After six unsuccessful attempts to log on to an information resource, the logon ID or account must be suspended for a period of at least 15 minutes or until the system administrator resets the password.

Reset Passwords

Users with non-privileged accounts who have forgotten their passwords can reset their password with the exception of privileged, machine and vendor default accounts.

The user shall be required authenticate prior to being allowed to perform password reset.

Password change requests via Help Desk shall be documented via change request ticket. Such a password shall be reset to a temporary password by an administrative group, and the user must then change the password at first logon.

Password Expiration

All MOH IT resources must offer an authentication information-aging feature that requires users to periodically change passwords.

All personnel must change their passwords when prompted by the system. Password expiration requirements are as follows:

a) Prior to the expiration passwords, the information resource provides notification to the user.
b) At least every 30 days, passwords for privileged accounts or for those accounts considered sensitive (e.g., system supervisors, software specialists, system administrators, or vendor-supplied) must be changed.
c) At least every 90 days, passwords for all other accounts must be aged and changed.

Non-expiring Password Accounts

All requests for use of non-expiring password accounts must be submitted in writing by the information systems owner to the Head ICT. These accounts shall be tracked for compliance purposes. Where approval is granted, the following compensating controls must be implemented:

a) Account must be in a centrally managed database with non-privileged access allowed.
b) Encrypt the password database to keep the password from being transmitted across the network in clear text.
c) Change password when personnel with access to the account leave or transfer.
d) Rights and privileges of non-expiring password accounts must be reviewed at least on a semi-annual basis to evaluate the appropriateness of access.

e) Passwords for non-expiring password accounts should comply with password complexity requirements.
f) Source-restrict the account to a specific host and do not allow console or remote entry.
g) Restrict access to the password to operations staff with a need to know.

Password Protection

Passwords used to connect to MOH IT resources must be treated as sensitive information and not be disclosed to anyone other than the authorized user, including system administrators and technical support staff.

Requirements for protecting passwords include the following:

a) Passwords must not be shared.
b) If passwords are written down and stored outside the user's personal control, they must be secured in a tamper-resistant manner (e.g., an envelope with registry seal, time stamped, and signed by the user) to ensure that any disclosure or removal of the written password is clearly recognizable.
c) If there is reason to believe that a password has been disclosed or otherwise compromised, the user must immediately change the password.
d) Passwords in transit must be encrypted.

Password Storage

Passwords must be stored in one-way encrypted format. This includes passwords stored in batch files, automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems.

Vendor Default Passwords

Vendor-supplied default accounts must be disabled, removed, or the passwords must be changed before connecting the system or introducing the software to the MOH information technology network. This applies to passwords used by contractors or consultants when configuring a system.

Data Security

Data in the health sector is generated at the health facilities and is shared with the other levels of the healthcare system. Due to its sensitive nature, data should be protected by policies, rules and regulations to safeguard it from losses and misuse. Data is transmitted by use of manual or electronic forms/modes

Information systems should have clear policies that define how data is captured, accessed, stored, modified, transmitted, and archived/destroyed.

All staff using the information system should adhere to the following information security requirements:

- Authentication
- Accountability
- Identification
- Authorization
- Integrity
- Confidentiality
- Availability
- Security Administration
- Audit

Data Access

Systems should ensure that electronic records are safeguarded against unauthorised access by incorporating the following security level areas that include but not limited to authentication, data integrity, system security and internet security

Access to patient level-data should be limited to only to authorized person as per existing regulations and should maintain audit trails of the users and service providers for easier management of the access processes.

The systems deployed in the health sector should ensure that they have distinct user access levels based on the user's responsibilities. All accounts should be documented and administered in a secure manner with considerations given on the risks inherent with each account type.

Access to patient-level data for use other than treatment shall be subject to the relevant laws and regulations.

Database management systems should ensure that they comply with security policies that includes;

- Role based access
- Authentication of all access by information resources, administrators and users
- Prohibit all unauthorised database manipulations
- Prohibit all unauthorised access to database servers

Enforcement of the following controls should be considered in order to support data access guidelines requirements:

- Use of menus to control access to application system function;
- Only provide access to system documentation on a need to know basis;
- Enforcing the minimum access capabilities (read, write, execute, create and delete) needed by users to meet their requirements;
- Ensure that output from application systems which handle sensitive data contain only the data that are relevant to the use of the output.

Data Interchange

All systems should exhibit properties of being interoperable with other existing systems by ensuring that they support data interchange standards such as HL7, SNOMED, DICOM, PACS, LOINC and SDMX among others.

Data Backups and Archival

System users should ensure that proper backup of data is done at all levels to ensure system recovery in case of failure or theft to data and transmission equipment. The system administrator should ensure that there exists clear back up policies and procedures.

Data Encryption

Any sensitive information stored on removable devices or media must be encrypted and stored in a controlled area. Sensitive information that is stored outside MoH premises must be encrypted and stored in a controlled area as well.

Some level of system and data security should be implemented by way of data encryption and passwords in all health systems dealing with patient level data to safeguard it from accidental/unauthorised access from malicious people. Applications should support end points encryption to ensure that data security.

Network Security and Access

The MoH network infrastructure must be protected at all levels commensurate with its value to the health sector. Such protection must include the implementation of the physical, administrative, and technical security controls and processes that safeguard the confidentiality, availability, and integrity of the network.

Network controls and processes are necessary to ensure the following:

a. Safeguard data traffic;

b. Detect and prevent unauthorized access;

c. Respond to computer security incidents;

d. Detect and correct transmission line errors;

e. Ensure message integrity throughout the Network;

f. Ensure that recovery procedures are in place and working;

g. Specify the appropriate auditing procedures.

Scope

All transmission of information used on behalf of MoH over local area networks (LANs); wide area networks (WANs); voice communications; videoconferencing systems; voice messaging systems; desktop video communications; satellite broadcasts; facsimile transmission; and all other transmissions over landline, wireless, or Internet-based network property .

All types of information and network services, data, voice, image, and multimedia communications, regardless of transmission technology.

Guidelines

The ICT unit prohibits the attachment of any non-approved network devices such as routers, switches, repeaters, wireless access-points, and firewalls to any point of the network. The ICT unit shall remove or disable non-approved network devices added to the network infrastructure.

The network infrastructure — facilities, equipment, services, protocols, and applications used to transmit, store, and process information — must be protected through the enforcement of the following controls;

a. Physical security

b. Network asset control

c. Network configuration information

d. Identification and authentication

e. Authorization.

f. Hardening standards

g. Secure enclaves

h. Network isolation (Demilitarized zones)

i. Penetration testing and vulnerability assessments.

j. Firewalls

k. Routing and switching services

l. Network traffic monitoring

m. Remote access controls

n. Network audit logs

Enforcement of network controls

Physical Security

Access to network infrastructure components must be limited to authorized personnel. Components of MoH networks must be located in areas secured to a level commensurate with the sensitivity of the information transmitted.

Network Asset Control

All infrastructure components must be inventoried at regular intervals and labeled for asset management and physical protection.

Network Configuration Information

Network information, including, but not limited to, configurations, addresses, subnet masks, secure enclave locations, and firewalls must be protected and treated as sensitive information. Access to network configuration information must be based upon the security principles of need to know and least privilege.

Identification and Authentication

Personnel must be required to identify and authenticate themselves to the network before being allowed to perform any other actions on the network.

Authorization

Access to information resources must be granted based on the job function, appropriate clearance, need to know, separation of duties, and least privilege.

Hardening of Information Resources

Hardening refers to the process of implementing additional software and hardware security controls. Information resources supported by networking must be hardened to meet or exceed the requirements specific to each platform.

Secure Enclaves

Enclaves can be implemented to enforce separate security zones (e.g., to segregate information resources with similar issues and risks). All traffic in and out of the enclave is forced through a control interface. Enclaves can be implemented as required, for instance, where;

a. Information resources accessible from the Internet

b. Patient protected data information, and

c. Sensitive and critical information resources whose risks warrant additional protection.

Network isolation (Demilitarized zones)

Secure network enclaves are areas where special protection and access controls, such as firewalls and routers, are utilized to secure information resources. Secure enclaves apply security rules consistently and protect multiple systems across application boundaries. Where possible regional offices should employ appropriate network channel encryption either at endpoints or at application level to secure transmission of sensitive information. Secure enclaves can be implemented using;

a. Servers within the network based on the sensitivity of the data.

b. Network segments (subnets) separate from the remainder of MoH information technology service networks.

c. Packet filtering or application proxy firewalls, to mediate and control traffic.

d. Intrusion detection systems and intrusion prevention systems.

e. Restrict sharing of physical devices among multiple enclaves.

Network Access & Connections

There must be approval by ICT unit in advance for the establishment of network connectivity. Any connectivity to the MoH network must allow monitoring.

Third-Party Network Services

Network services approved for third-party connectivity must be governed by the principle of least privilege and limited to those services and devices needed to perform the business function requested.

When establishing third-party connections, access controls and administrative procedures must be implemented to protect the confidentiality of MoH information. The third party must be responsible for protecting its private network infrastructure and information and must not rely on the MoH information technology to perform this function.

Remote Access Controls

Remote access privileges are restricted to authorized personnel and must be approved by appropriate management before being granted. The use of personal information resources to remotely connect to the MoH intranet must be approved and connectivity must be managed through an approved virtual private network (VPN) solution.

Remote access should require users or devices to authenticate at the perimeter or connect through a firewall. Remote user communications must occur through VPN or appropriate encrypted channels.

To protect the integrity of the MoH information technology environment, use of remote administration and maintenance software and associated security controls must be approved.

Telecommuting

Personnel working at alternative work sites must only use MoH information technology approved computer hardware, software when working on MoH business. Any approved personal hardware must have appropriate security protection, personal firewall and meet security policies on the domain.

Network Audit and Compliance monitoring

Networks including firewalls and controlled interfaces must have an audit capability to create, maintain, and protect an audit trail from modification or unauthorized access or destruction. Network audit logs must include the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of network integrity.

For events where immediate attention is required, the audit utility must trigger alarms that are directed to the proper location for action. Network audit logs must be reviewed periodically for potential security incidents and security breaches. Audit logs may be reviewed to evaluate the damage caused by a security breach and support the recovery of data lost or modified.

The ICT Unit will perform continuous monitoring of the network using appropriate hardware and software techniques. Periodic checks will be performed to identify rogue access points and possible unauthorized access.

Only authorized personnel may perform monitoring and audit compliance to network standards and guidelines, hardware and software requirements. Dedicated network monitoring undertaken shall cater for traffic analysis of wired and wireless security issues and respond appropriately.

`

Firewalls

Firewalls define perimeters that control the traffic between MoH network and other networks. All inbound or outbound network traffic is controlled by firewalls, settings on the appropriate access control devices, such as routers.

All connections to any network(s) other than the intranet must be controlled by firewalls managed by MoH ICT unit.

Network pen-tests and vulnerability assessments

Security assessments and audits are essential tools for checking the security posture of network and for determining corrective action to ensure the network remains secure. Administrators should periodically check for rogue access points and against other unauthorized access.

Only authorized personnel may use diagnostic hardware and software that enable the bypass of implemented security features or allow network monitoring (e.g., network scanning and sniffers). Dedicated wireless monitoring that performs a full traffic analysis must be implemented to identify wired and wireless security issues and respond appropriately.

Server rooms Standards and guidelines

Server rooms shall generally house servers, backup and the necessary network electronics for establishing a local computer network in the server room.

In all cases, the server room serves as a centralized operations center for processing, storage, and transmission of data

As a result of high density of equipment and cabling, Server room design and operations must place particular emphasis on such factors as:

- Adequate facility Space
- Power Supply (operational and backup)
- Cooling (general and rack-specific)
- Cabling pathways
- Equipment racks
- Cabling system (components and design)
- Personnel Conduct

`

Scope

The scope of these guidelines is to aid in the design and implementation of Server rooms and similar facilities, such as dedicated computer rooms.

Facility Spaces

Although equipment cabinets are similar in appearance and dimensions, their contents determine where they are located within the data center. The types of network devices commonly associated with data center cabinets include:

- Servers
- Storage devices
- Switches (general network, server cluster, storage network, management)
- Load balancers
- Routers
- Special-purpose appliances (security, acceleration)

Additional space requirements

To fully support Server Room operations, the following service rooms and access points should be catered for in the overall server room design;

- Office space for server room support staff
- Network Operations Center (NOC) to monitor and manage server room devices and traffic
- Electrical and mechanical rooms
- Storage room for parts and equipment
- Configuration/staging room to test and prepare devices for deployment
- Shipping/receiving room
- Secondary entrance room for supplemental or backup communications circuits to access providers

`

Server Room Requirements

Server rooms should meet the following minimum criteria:

Architectural design

- Location; must be housed in a secure location
- Ceiling height; must provide sufficient ceiling height
- Have a raised floor systems

Environmental

The Server room environment shall be controlled with particular emphasis being on the following areas:

- Cooling
- Fire suppression system
- Water/Smoke detectors
- Alarms systems

Electrical

- Stand by power i.e. provision of generators, UPS, batteries
- Grounding/proper earthling

Structured cabling

- Flexible cabling system to handle a wide range of current and future technologies(LAN, WAN,SAN)

Guidelines for equipment placement

- Firefighting equipment this equipment should be placed in an easily accessible location.
- Power/stabilizer room this should be a separate room hosting batteries, to provide power in case of power outage
- Operation room this a room set aside for local data Centre/server room background operation and maintenance

`

Remote operational center

- Systems to enable remote operations of the server room should be put in place to ensure that most maintenance functions are carried out remotely.

Security and availability considerations

These following guidelines should ensure the server room's security and availability for day-to-day operations

- Entrances & Exits must be controlled and monitored through electronic surveillance
- Resources for fire prevention, detection, suppression, and containment must be adequately installed
- Preparedness for damaging climactic events (floods, lightning strikes))
- Redundant/failover spaces, pathways, cabling, power, network devices
- Communications links
- Ensure staff have access to and understand the security policies on: Third-party or customer system access; Security violations; Auditing; and System access controls

Pathways

The server room design should allow for adequate space to minimize interference between the following services;

- Air circulation pathways
- Power cable pathways
- Network cable pathways

Personnel Conduct and Prohibited Items

Personnel accessing the server rooms are required to adhere to the following;

- All personnel shall act in a professional manner.
- Smoking is prohibited inside the Server Room.
- Security badges shall be worn conspicuously above the waist.

The following items are strictly prohibited in the server rooms

- Instruments or materials likely to produce substantial injury or damage to persons or property (e.g. Explosives and dangerous weapons).

`

- Controlled substances (e.g. illegal drugs and associated paraphernalia but not prescription medicine).
- Any other item prohibited by law.

Server Room Operation procedures

These procedures shall be used in the access control of the server room and equipment in the server room.

Access

1. Only authorized users should be allowed into the server room and they should have their identification cards at all times
2. All equipment in the server room should have access control measures in place; they should have user names and passwords authentication modes to the least.
3. There should be periodic security risk assessment of the server room and all equipment.
4. A designated officer should be a custodian of security codes and related keys at all times.
5. All authorized visitors into the server room should be accompanied by authorized personnel.
6. Server rooms should be monitored by intruder detection systems that are monitored by the security personnel.

Power management

1. There should be clean power into the server room
2. There should be power backup alternatives
3. There should be route cables between equipment and to patch panels. Trailing cables across floor areas shall not be permitted.

All environment appropriate standards should be adhered to in server room.

Equipment change control

When installing new equipment to the server room infrastructural farm the following procedure should be followed:

1. Plan on the integration of the new equipment and inform users that maybe affected by the new equipment installation.
2. Install the appropriate operating system and application software.

3. Configure the appropriate security configurations as per the server room's SOPs
4. Add the equipment into the existing infrastructure during low traffic hours to avoid downtimes. Ensure no services are interfered with by inclusion of the new equipment.
5. Monitor operation of the new equipment during high traffic hours

System/software change control

1. An assessment should be done on the existing hardware and other ICT resources in the server room that are to be used in a software/system change.
2. Install the appropriate operating system and application software. Configure the appropriate security configurations as per the server room's SOPs
3. Monitor the new software and how it integrate into the existing system

Configuration management

1. Establish and maintain baseline configurations and inventories of organizational information systems including documentation throughout the respective system development life cycles
2. Establish and enforce security configuration settings for information technology products employed in organizational information system.

Backup and Disaster recovery

There should be a documented backup procedure on network equipment configurations, server configurations, and applications and databases. The procedures should be stored on-site and off-site.

BACKUP AND DATA RECOVERY GUIDELINES

Data is one of the most important assets to the Ministry of Health. In order to protect data loss or destruction, it is imperative that data is efficiently and securely captured, processed, and stored. Backup and data recovery guidelines shall govern data backup and restoration for ministry servers, user desktops, PCs and mobile devices. In addition, the guidelines address modalities for restoration of backed up data to individual systems.

Different approaches may be used to curtail data loss and increase the availability of data for local and alternate site recovery. The technologies used must provide for both backup and recovery to meet local requirements in addition to making data available at alternate processing site for disaster recovery.

The Ministry of Health shall adopt the following levels for data backup and recovery.

Level 1: Automated Central Server Backup

Automated central server backup guidelines cover backup of data that resides on MoH servers located at national and regional offices.

What to Back Up

Backups shall include; data, databases, email, operating systems, configuration files, general utilities, application software, supporting files and tables, scripts, standard operating procedures, specialized equipment, and related documentation.

When to Back Up

Backup shall be undertaken;

a) Prior to migrating system to test or production and prior to maintenance.
b) After migrating to production and after maintenance environment.
c) After update by batch processing and the successful completion of the update.
d) After update by real-time processes at a frequency based on the recovery time and recovery point of the application.

Backup Schedules

All essential components must be backed up on a schedule that is sufficient to meet the recovery time of the application or information resource as defined.

Server backups should be done automatically. Backup job failures must be properly documented, investigated, and remediated in a timely fashion.

The following are the recommended backup schedules;

a) Real-time backup for mission critical applications and data.

`

b) Scheduled periodic backup based on set recovery point and whenever application changes are made for Operating systems, configuration files, general utilities, application software.
c) Incremental backup on weekly basis or as appropriate for archive data.
d) Full quarterly backups for standard operating procedures, equipment documentation, and manuals.

Backup Administration

Server administrators shall ensure that all new servers are added to the backup schedule and that the schedule is applied to each new server's maintenance routine.

Prior to making a system change such as deployment of a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed.

Prior to retiring a server, a full backup must be performed and placed in secure permanent storage.

Backup media types

Media for backup shall include;

a) Tape vaulting (periodic or real-time)
b) Managed optical disk storage (periodic automated backup)
c) Managed network storage for database and journals (real-time)

Backup media must be securely stored in a fireproof container at the facility that hosts the application and a copy kept off site.

Backup shall adhere to a naming convention that aids the easy identification of the backup based on the timestamps, name of server, and application. The ICT Unit shall come up with guidelines for the naming convention.

Backup Inventory

An inventory of critical applications backup media and supporting materials must be maintained. A copy of the inventory must be securely stored off site or in a fireproof container at the facility that hosts the application.

It is recommended that an inventory of backup media and materials is recommended for all other information resources.

Level 2: Distributed Data Backup

This category applies where backup is undertaken where no specialized backup equipment, servers and media is available to carry out this function. In this environment backup may not be automated, centralized or a dedicated backup administration provided. A PC may be designated as the backup server to carry out backup at regional offices.

To the greatest extent possible the guidelines provided under Level 1 on backup schedule, backup administration, and backup inventorying shall apply for distributed data backup.

Level 3: End User Backup

Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data to the appropriate server provided for this purpose in order that their data is backed up regularly. End users shall follow the appropriate data backup regimes defined in Level 1 backup category.

End users ought to save and close all files, as well as all related applications, prior to commencing backup.

The ICT unit shall endeavor to create awareness on data backup practices and procedure as necessary for end users.

Conducting End user Backup

Local user backups must be conducted once every 30 day(s).End user backups can be conducted manually or automatically. For automated end user backup, a tool shall be provided by ICT unit.

Alternate Backup Requirements

All information resources not using one of the above recommended backup technologies must implement alternative secure backups. The information resource must have the capability to check the integrity of data read from a backup file when performing a restore function.

Data Restoration

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. It is essential to regularly test the ability to restore data from its storage media.

Data restoration shall ensure that;

a) All daily backup media must be tested at least once every month to ensure that the data they contain can be completely restored.
b) All weekly backup media must be tested at least once every 3 months to ensure that the data they contain can be completely restored.
c) All monthly backup media must be tested at least once a year to ensure that the data they contain can be completely restored.

Data Restoration Guidelines

In the event a data restore is required, the following guidelines shall be adhered to:

a) The individual responsible for overseeing backup and restore procedures shall fill and submit a request form that is duly authorized and documented.
b) In the event of unplanned downtime, attack, or disaster, the full restoration procedures contained in *Disaster Recovery Plan* must be followed.
c) In the event of a local data loss, the end user affected must contact the ICT unit and request a data restore as soon as practical.

`

d) Depending on the level of data loss; a daily, weekly restore media or combination of both will be used.
e) The media must be retrieved by the server administrator based on a pre-determined replacement procedure. If media is offsite and the restore is not urgent, then the end user/s affected may be required to wait for an appropriate time for the media to be retrieved.

Personnel Security Training

To help realize the security standards and guidelines, ICT personnel must be trained in the following areas:

a) System and security controls
b) Data backup and recovery
c) Acceptable use of electronic systems
d) Server room operation and maintenance

CAPACITY BUILDING/ICT HUMAN RESOURCE DEVELOPMENT

Introduction

The development and implementation of these guidelines are subject to the existing rules, regulations and policies governing human resource development in the Ministry.
Most of the health providers have not embraced ICT in the health service provision; this therefore poses a significant challenge in building ICT capacity in the health sector since most training programs do not currently include ICT in their course content.

Objectives

The human resource aspect of ICT is to ensure that the Ministry staffs are able to:

i. Provide effective and efficient support in the development and maintenance of ICT;
ii. Use ICT to support efficient and effective healthcare service delivery;
iii. Innovate and apply new technology consistent with ICT trends
iv. Promote the use of ICT enabled services within the ministry

Scope

These guidelines apply to any person accessing or using the ICT infrastructure, managed, supported, or operated by, or on behalf of the Ministry of health.

The guidelines specify the general approach to the training of all staff and stakeholders accessing the Ministry's ICT services as primary users.

Roles and responsibilities

i. The head of ICT will liaise with the mandated training committee in the Ministry in the determination of overall ICT training needs and capacity building for the Ministry employees;
ii. The Ministry shall encourage employees to acquire necessary ICT capabilities skills for use of ICT resources;
iii. The ministry shall design client-centered skills development plan consistent with the overall strategic plan and Human Resource Development standards and guidelines; policy of the Government.
iv. The ministry shall continuously monitor the implementation of training plan/human resource development plan.
v. ICT trainings shall factor in the qualitative and quantitative aspects of training as well as instilling basic ICT knowledge and skills to the staff.

`

Levels of training

Classifications of users based on needs

- ICT technical staff
- Managers
- General users

Modes of training

The ministry shall support the following modes of training;

Internal

Based on the departmental/divisional recommendations, the ministry shall conduct internal ICT training on a continuous basis through On Job Training (OJT) and workshops

External training

Where training cannot be conducted internally, the ministry shall organize external ICT training in response to the needs and recommendations of the departments.

ICT literacy

The training should be in line with the demands of the job functions of the trainees. The training shall therefore focus on building skills in users making them effective in exploiting provided ICT resources.

Training Resources

- The Ministry shall ensure that adequate resources are availed for ICT training in the budget.
- Departments shall be encouraged to continuously carry out ICT training needs assessment of their staff in order to prioritize on the available resources to ensure that the resources are used efficiently and effectively
- Training materials shall be availed to participants in appropriate format (e.g. electronic media)

Nomination of trainees

a) The ICT shall liaise with the HRD to develop an annual training schedule

b) Departmental heads shall initiate the nomination of participants for internal training

`

c) Where the internal training cannot meet the needs of the departmental staff, external training support shall be provided to selected staff
d) A knowledge transfer mechanism shall be adopted
e) Mentorship programs shall be encouraged
f) An agreed upon selection for the participants criteria should be developed in consultation with Divisional/ Departmental MTC

Certification/Acknowledgement of training

Ministry shall demand that employees supported for ICT training produce evidence of participation in such trainings through certificates, etc.
Training agents/coordinators shall be required to submit certified attendance list
The ICT unit shall device metrics to measure the effectiveness of training programs and monitor the same constantly to ensure that the desired levels of learning are achieved. Such metrics could include but not limited to work plans etc.
Continuous professional education (CPE) shall be encouraged to ensure that all ICT technical staff maintains an adequate level of current knowledge and proficiency in the field of information technology.
The Ministry shall endeavor to partner with academic institutions for training programs where necessary.

`

MONITORING AND EVALUATION

All ICT systems are the property of MOH. The MOH therefore reserves the right to monitor these systems to ensure compliance with this standard. The monitoring of the ICT system activities will be carried out in a manner that respects the rights and legitimate interests of those concerned.

(i) Users of the MOH ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy. In order to maintain their privacy, users of the MOH ICT resources should avoid storing private information. By using the MOH ICT systems, users expressly consent to the monitoring of all their activities within the MOH's ICT systems.

(ii) During the implementation of this standard MOH will ensure that there is continuous monitoring and evaluation for efficiency, accountability and transparency. The Monitoring and Evaluation will be carried out by the ICT internal M&E team in consultation with the MOH M&E Technical Committee.

Compliance

All users of the MOH ICT systems are required to read the ICT standards and adhere to the guidelines in this document.

Review

This standard will be regularly reviewed and amended as required to ensure it remains relevant and effective in meeting its objectives. The responsibility for the ongoing review resides with the head of ICT in conjunction with the ICT Governance Committee. Any changes to this standards and guidelines shall be communicated to all users of the MOH ICT systems. Monitoring of the use of the standards will be done every quarter

Adherence of the standards indicators;

- %age of health institutions using ICT (by type of health institution: e.g. private clinic, government etc.)
- Regional distribution of health institution with computers, telephones and internet connectivity
- %age of health professional that use ICTs for medical purposes
- Ratio of availability of personal computers to number of staff
- %age of officers accessing internet
- %age of government offices and agencies with a web site
- Security
- %age of doctors that use ICTs for medical purposes (research, telemedicine, And E-mail etc.) By type of ICT (computer, Internet)
- %age of health institutions using ICTs (by type of health institution: Private clinic, government, university hospital, pharmacy etc. and type of ICT)

`

REFERENCES

Kenya National e-Health Strategy 2011-2017. *Ministry of Medical Services and Ministry of Public Health & Sanitation*. April, 2011.

E-Government Strategy 2011-2014. *Directorate of e-Government*, February 2011.

ICT Standards and Guidelines. *Directorate of e-Government*, March 2011.

Standards and Guidelines for Electronic Medical Record Systems in Kenya. *Ministry of Medical Services and Ministry of Public Health & Sanitation.* September, 2011.

Kenya Health Policy 2012-2030*. Ministry of Medical Services and Ministry of Public Health & Sanitation.* September, 2011.

National Information & Communications Technology (ICT) Policy. *Ministry of Information & Communications.* January, 2006.

ICT Standards in the Health Sector: Current Situation and Prospects - A Sectorial e-Business Watch Study Final Report (Version 3.0). *European Union*, June 2008.

ISO 9126- 1 Software product quality, ISO/IEC 9126-2 on External usability metrics , ISO/IEC 9126-3 on Internal usability metrics, ISO/IEC 9126-4 on Quality in use Metrics, ISO 9241-11 Guidance on usability, ISO 14598 – 1 on Software product evaluation, ISO 27799 – Information security management in health using ISO/IES 27002

ISO 27001-2 **standards** for security management and Information security

ISO/TS 29585:2010 Health Informatics standards

`

Annexures

Table1. SWOT Analysis

Strength	**Weakness**
• ICT skilled human resource at both the National and County Levels • There are policies guidelines by other Ministries that guide the Ministry of Health • Availability of fiber connectivity at both National and County levels. • Availability of ICT infrastructure at the Ministry of Health National Level and e-government data centers	• Limited ICT skilled man power • Limited resources for ICT projects • Lack of dissemination and adherence to ICT standards and guidelines from e-government • Inadequate ICT use skills of staff in all levels of healthcare provision • Lack of ICT infrastructure at all levels of healthcare provision • Lack of Fiber connectivity to the regional offices and health facilities • Health care data is sensitive hence require particular policies on data management on Information System
Opportunities	**Threats**
• Resources to invest in ICT projects; finances from partners to support • Top management support in the ministry • Opportunities for training of staff • High ICT enthusiasm of the health workers at all levels, receptive • Availability of ICT technologies to support health care service delivery	• Low and non-existing ICT staff at the regional and lower levels of health care system • Poor linkage of ICT projects at the National Level programs • Stakeholders conflict of interest on ICT projects for health care provision

The table below summarizes as SWOT analysis of MoH ICT unit

`

Table2: Software Development Life Cycle

The table below summarizes the different phases in a software development life cycle

Phase	Activity	Deliverable	Responsibility
Phase-1: Problem Identification /Project Initiation	• Identification of gaps within existing systems	• Constitution of relevant team to analyse the problem • Determine impact of problem • Suggest viable solution options	• ICT personnel • Relevant stakeholders
Phase-2: Feasibility Analysis/ Information Gathering	• Assess implications (Economic, technical, social, Operational, ethical)	• Feasibility analysis report	• Steering committee
Phase-3: Systems Analysis	• Identify Users, inputs, processes, outputs, desired platforms) • Required functionalities • Hardware requirements • Human resource	• Detailed specifications requirements document • Detailed budgets	• Stakeholders • Steering Committee • ICT Unit
Phase-4: Systems Design/Logical Design	• System modelling	• Data flow diagrams/Algorithms • System interfaces • Logical interfaces • Entity Relationship Diagrams	• ICT • Development teams
Phase-5: Development/Coding	• Programming	• System Modules	• ICT/ Development team
Phase-6: Testing	• System testing using dummy data	• Reviewed test report	• ICT/development team • Selected users
Phase-7: Implementation	• Installation • Change management • Technical and user training • Commissioning	• Functional System • Stakeholder acceptance • Handover reports • System usability	All stakeholders
Phase-8: Post Implementation Review	• System and User evaluations • Notify stakeholders • Determine satisfaction • Close the request	• Impacts on processes • Request closed	Management/ ICT
Phase-9: Maintenance	• System maintenance plan	• Service level agreements • Maintenance schedules	Management/ ICT

`

Table3: List of the Technical contributors to ICT Standards and Guidelines Technical Contributors

SNo.	Name	Designation	Organization
1.	Dr. Samuel Were	Head, Technical Planning	Ministry of Public Health and Sanitation
2.	Dr. Esther Ogara	Head, e-Health,	Ministry of Medical Services
3.	Mr. James Njiru	Head, ICT	Ministry of Public Health & Sanitation
4.	Mr. Edwin Kemboi	Head, ICT	Ministry of Medical Services
5.	Ms. Anne Barsigo	Chief of Party	Futures Group
6.	Mr. Joshua Oiro	Deputy Chief of Party	Futures Group
7.	Mr. Ali Karisa Juma	Senior Technical Manager	Futures Group
8.	Mr. Mwenda Gitonga	Senior Technical Manager	Futures Group
9.	Ms. Rachael Wanjiru	Senior ICT Officer	Ministry of Public Health and Sanitation
10.	Mr. Nicholas Ngari	ICT Officer,	Ministry of Medical Services
11.	Mr Bethwel Cheruiyot	ICT Manager	Moi Teaching and Referral Hospital
12.	Ms Eunice Awuor	ICT Officer	Directorate of e-Government
13.	Mr. Edward Tuitoek	ICT Officer	Ministry of Public Health and Sanitation
14.	Mr. Ajwang	ICT Officer	Directorate of e-Government
14.	Josiah Korir	Principal ICT Officer	Directorate of e-Government
15	Nelly	ICT Officer	Ministy of Medical Services
16	Phillip Ochieng	ICT Officer	Ministry of Public Health and Sanitation
17	Monica Wambui	ICT Officer	Ministry of Public Health and Sanitation

`

REPUBLIC OF KENYA

Ministry of Health,
Afya House, Cathedral Road,
P.O. Box: 30016-00100,
Nairobi, Kenya.
Tel: +254 020 717077
Email: enquiries@health.go.ke
ps@health.go.ke

KENYANS AND AMERICANS
IN PARTNERSHIP TO FIGHT HIV/AIDS

CENTERS FOR DISEASE CONTROL AND PREVENTION

Futures GROUP