Republic of Zambia

Ministry of Health

Information & Communication Technology Standards and Guidelines

January 2014

Directorate of Policy and Planning
Information & Communications Technology Unit
Haile Sellaise Avenue
Ndeke House
P. O. Box 30205
LUSAKA

info@moh.gov.zm
www.moh.gov.zm

FOREWORD

This document establishes the Information & Communications Technology Standards and Guidelines for the Ministry of Health. The Ministry of Health is responsible for health in this country and it has embraced ICTs as an integral tool in its quest to deliver quality health services as close to the family as possible. These guidelines do not only prescribe the standards for hardware and software to be used in the Ministry of Health and its institutions, but also outlines the information communications technologies available in the 21st Century.

The guidelines also provide a framework to leverage the application and exploitation of cutting edge ICT technologies in the health care delivery system.

The Information and Communications Technology Standards and Guidelines are therefore intended to give guidance on the procurement, usage, maintenance and safe disposal of all ICT hardware and software in order to ensure appropriate standards and guidelines are followed and adhered to.

Users of these guidelines are encouraged to send feedback to the ICT Unit on their utilitisation and content to assist in their future development. This shall help the Unit to ensure that standards and guidelines evolve to meet emerging requirements.

Hon. Dr. Joseph Kasonde, MP
MINISTER OF HEALTH

ACKNOWLEDGEMENTS

The Information & Communications Technology Standards and Guidelines for the Ministry of Health were developed out of a need to standardise the operations and use of the ICTs in the Ministry.

The ICT Standards and Guidelines have been developed in accordance with the National Information and Communication Technology Policy of 2010.

On behalf of the Ministry of Health, I would like to acknowledge the commitment, hard work and in a special way thank the following people who devoted their time in ensuring that this manual was developed:

Dr. Christopher Simoonga	-	MoH: Director – Directorate of Policy and Planning
Mrs Christine Mshanga	-	MoH: Director – Human Resource and Administration
Mr Paul Mumba	-	MoH: Assistant Director – Policy
Mr. Chipalo Kaliki	-	MoH: Assistant Director – Monitoring and Evaluation
Mr. Noel Masese	-	MoH: Assistant Director – ICT
Mrs Matildah M. Zyambo	-	MoH: Head – Procurement and Supplies Unit
Ms Namataa Kalaluka	-	MoH: Chief Accountant
Mrs Nora Sichilongo	-	MoH: Principal Internal Auditor
Mr. Rutendo Chitembure	-	MoH: Principal ICT Officer - Software
Mr. Andrew Kashoka	-	MoH: Principal ICT Officer – Hardware and Networks
Mr. Trust Mufune	-	MoH: Principal Monitoring & Evaluation Officer
Ms. Virginia Simushi	-	MoH: Senior ICT Officer
Mr. Richard Tumeo	-	MoH: Senior ICT Officer
Mrs Sheila Mumbi	-	MoH: Senior ICT Officer
Mr. Innocent Chiboma	-	MoH: Senior ICT Officer
Mr. Moses Mutabwa	-	MoH: ICT Officer
Mr. Levison Nkhoma	-	MoH: ICT Officer
Mr. Kenneth Chanda	-	MoH: ICT Officer-Information & Website Management
Mr. Zanga Sikazwe	-	MoH: SmartCare Data Analyst
Mr. Chisanga Siwale	-	MoH: SmartCare Data Analyst
Mr. David Nchinga	-	UTH: Ag. Senior Systems Analyst
Mr. Paul Chima	-	UTH: Computer Operator
Mr. Samson Phiri	-	Copperbelt: Provincial ICT Officer
Mr. Dipo Mbewe	-	Lusaka: Provincial ICT Officer
Mr. Caleb Milambo	-	Southern: Provincial ICT Officer

Mr. Prince Munyati	-	Central: Provincial ICT Officer
Mr. John Kabwe	-	Northern: Provincial ICT Officer
Mr. Moffat Zulu	-	North Western: Provincial ICT Officer
Mr. Chalwe Chalwe	-	Chainama Hospital: Ag. Systems Analyst
Mr. Kennedy Sakala	-	Chainama College: Ag. Systems Analyst
Mr. Brain Ntentabunga	-	LMGH: ICT Officer - Networks
Mr. Sipopa Mulikita	-	LMGH: ICT Officer - Hardware
Mr Chiza Banda	-	NCH: Systems Analyst
Mr. Chipopa Kazuma	-	MSL: Project Manager
Mr. Brain Chibale	-	MSL: ICT Manager
Mr. Chris Opit	-	JSI: Senior ICT Advisor
Mr. Arthur Sichivula	-	ZAMRA: ICT Manager
Dr. Bwalya Chiteba	-	CDC: Health Informatics Branch
Mr. Stephen Ngala	-	CDC: Senior Network Engineer

Dr. Davy Misheck Chikamata
Permanent Secretary
MINISTRY OF HEALTH

TABLE OF CONTENTS

DEFINITIONS

Ministry of Health

All the departments, statutory boards and institutions under the MoH shall be referred to in this document as Ministry unless otherwise stated.

Information and Communication Technology (ICT)

A generic term used to express the convergence of telecommunications, information, broadcasting and communications such as computers and the internet, fixed and mobile telephone, high frequency radio, radio and television and related applications such as email, voicemail and Voice over Internet Protocol.

ICT Infrastructure

A generic term to mean computer hardware and peripheral devices, communication equipment including networks.

ICT Resources

All the MoH Information and Communication Technology resources, consultancy services and facilities including, but not limited to: mail, telephone, mobile phones, voice mail, Short Message Service (SMS), facsimile machines, email, the Intranet, computers, printers, scanners, access to patient records, including Information Systems such as HMIS, FAMS, EHR or other facilities that the MoH owns, leases or uses under license or by agreement, or the use of any part of the MoH network to access other networks.

Users

All employees and any persons authorised to use the MoH ICT resources even those attached to MoH from other organisations including those invited to attend a course/ workshop at the MoH who have been granted access to, and use of, the MoH ICT resources.

A member of the public reading MoH web pages from outside the MoH offices is not by virtue of that activity considered to be a User.

Computer Virus

A computer virus is potentially malicious programming code that shall cause some unexpected or undesirable event to computer software, data and network interruption. Viruses can be transmitted via email or instant messaging attachments, downloadable internet files, USB disks, and CDs.

Workstation

A multicore multiple processor high specification PC.

Server

A server is a multicore multiple processor high specification computer that provides services to other computer programs and their users in a network environment.

Disaster Recovery

Disaster Recovery is the area of security planning that deals with protecting an organisation from the effects of significant negative events. Significant negative events, in this context, can include anything that puts organisation operations at risk; crippling cyber-attacks and equipment's failures as well as natural and man-made disasters.

Cloud Computing

The practice of using a network of remote servers hosted on internet to store, manage, and process data, rather than a local server or a personal computer. Organisations have data centres and they offer hosting facilities at a fee. The term cloud is essentially a metaphor for the internet.

ABBREVIATIONS AND ACRONYMS

ADF	Automatic Document Feeder
ART	Anti-Retroviral Treatment
BOYD	Bring Your Own Device
CD	Compact Disc
CDC	Center for Disease Control and Prevetion
CPU	Central Processing Unit
DHIS	District Health Information System
DHRA	Directorate of Human Resources and Administration
DMO	District Medical Office
DSL	Dedicated Service Line
DVD	Digital Versatile / Video Disc
EHR	Electronic Health Record
E-Mail	Electronic Mail
EMR	Electronic Medical Record
FAMS	Financial Management System
FTP	File Transfer Protocol
GB	Gigabyte
GHz	Gigahertz
HMIS	Health Management Information System
HRA	Human Resources and Administration
HRIS	Human Resources Information System

ICT	Information and Communications Technology
IFMIS	Integrated Financial Management Information System
IGC	Integrated Graphics Controller
ISDN	Integrated Services Digital Network
IWB	Interactive Whiteboard
JSI	John Snow Incorparated
LAN	Local Area Network
LCD	Liquid Crystal Display
LMGH	Levy Mwanawasa General Hospital
mHealth	Mobile Health
MoH	Ministry of Health
MSL	Medical Stores Limited
MTWSC	Ministry of Transport ,Works, Supply and Communications
NCH	Ndola Central Hospital
OS	Operating System
PABX	Private Automated Branch Exchange
PC	Personal Computer
PDF	Portable Document Format
PII	Personally Identifiable Information
PMO	Provincial Medical Office
PMTCT	Prevention of Mother to Child Transmission
PNG	Portable Network Graphics

RAM	Random Access Memory
SIM Card	Subscriber Identity Module Card
SLA	Service Level Agreement
SMS	Short Message Service
SSH	Secure Shell Protocol
SSL	Secure Socket Layer Protocol
USB	Universal Serial Bus
UTH	University Teaching Hospital
VoIP	Voice Over Internet protocol
VPN	Virtual Private Network
ZAMRA	Zambia Medicines Regulatory Authority
ZICTA	Zambia Information and Communications Technology Authority

1.0 INTRODUCTION AND BACKGROUND

The world today is influenced by the rapid development in information and communication technologies. ICT's have affected literally every sphere of human endeavour with connectivity playing a pivotal role in communication technologies. This rapid development has placed diverse obligations and responsibilities on how to effectively operationalise and maintain the information and communication infrastructure. The Ministry of Health therefore found it necessary to develop the Information & Communications Technology Standards and Guidelines to address many ICT concerns that shall enhance its mission of access to health care service as close to the family as possible.

The purpose of these guidelines is to define the standards for Information and Communication Technology and the infrastructure which supports the smooth operations of the ICT Unit in the Ministry, all its units and institutions.

Objective

The objective of these guidelines is to provide standards and rules for the sound management of ICTs for the Ministry, all its units and institutions.

The expected outputs of these standards and guidelines shall be:

a) Efficient and effective use of ICTs;
b) Prompt responses to ICT queries;
c) Adherence to set standards and guidelines.

2.0 PRINTER STANDARDS AND GUIDELINES

The ICT Unit maintains an inventory of printers in the Ministry. The maintenance of these printers shall be done by the Office Equipment Department under the Ministry of Transport, Works, Supply and Communications. However, where the Office Equipment Department is not available, a Service Level Agreement (SLA) should be entered-in for maintenance of printers with a reputable institution. The first line of support shall be provided by the ICT unit.

The Standards and Guidelines outlined in this document govern any requests for new printers in the Ministry.

1. All requests for new printers shall be made through the ICT Unit. The ICT Unit shall prepare a printer specification document.

2. All requests to move printers from allocated stations shall be made through the ICT Unit.
3. All installation and configuration of printers shall be undertaken by the ICT Unit.
4. All requests to move printers offsite shall be approved by ICT Unit before the items are released.
5. Damaged printers shall be replaced by the officer who collected them.

Guidelines:

1. All requests to move a printer shall be made at least one week prior to the date needed.
2. All printer specification shall be obtained from the ICT Unit.
3. All procured printers shall be checked for compliance to the specifications by the ICT Unit before installation.

2.1 Scanners Standards and Guidelines

The ICT Unit maintains an inventory of scanners in the Ministry. The maintenance of these scanners shall be done by the Office Equipment Department under the Ministry of Transport, Works, Supply and Communications. However, where the Office Equipment Department is not available, the SLA should be entered-in for maintenance of scanners with a reputable institution. The first line of support shall be provided by the ICT unit.

1. All requests for new scanners shall be made through the ICT Unit. The ICT Unit shall prepare a scanner specifications document.
2. All requests to move scanners from allocated stations shall be made through the ICT Unit.
3. All installation and configuration of scanners shall be undertaken by the ICT Unit.
4. All requests to move scanners offsite shall be approved by ICT Unit before the items are released.

Guidelines:

1. All requests to move a scanner shall be made to the ICT Unit at least one week prior to the date needed.
2. All scanner specifications shall be obtained from the ICT Unit.
3. All procured scanners shall be checked by the ICT Unit for compliance to the specifications by the ICT Unit before installation.

2.2 Projectors Standards and Guidelines

The ICT Unit maintains an inventory of projectors in the Ministry. The maintenance of these projectors shall be done by the Office Equipment Department under the Ministry of

Transport, Works, Supply and Communications. However, where the Office Equipment Department is not available, the SLA should be entered-in for maintenance of projectors with a reputable institution. The first line of support shall be provided by the ICT unit.

1. All requests for new projectors shall be made through the ICT Unit. The ICT Unit shall prepare a projector specifications document.
2. All requests to move projectors from allocated stations shall be made through the ICT Unit.
3. All installation and configuration of projectors shall be undertaken by the ICT Unit.
4. All requests to move projectors offsite shall be approved by ICT Unit before the items are released.
5. All meeting rooms shall preferably have a mounted and secured projector.

Guidelines:

1. All requests shall be received in the ICT Unit at least one week prior to the date needed.
2. All projector specifications shall be obtained from the ICT Unit.
3. All procured projectors shall be checked by the ICT Unit for compliance to the specifications before installation.

2.3 Laptops Standards and Guidelines

The ICT Unit maintains an inventory of laptops in the Ministry. The repair of these laptops shall be done by the Office Equipment Department under the Ministry of Transport, Works, Supply and Communications. However, where the Office Equipment Department is not available, the SLA should be entered-in for maintenance of laptops with a reputable institution. The first line of support shall be provided by the ICT unit.

1. All requests for new laptops shall be made through the ICT Unit. The ICT Unit shall prepare a laptop specifications document.
2. All laptops shall be branded and numbered according to Office Equipment Department under the Ministry of Transport, Works, Supply and Communications guidelines.
3. All installation of software and configuration of laptops shall be undertaken by the ICT Unit.
4. All laptops shall remain the property of the Ministry of Health and are not transferable to other ministries.
5. Laptops shall be procured with a laptop lock.
6. Laptops stolen at home shall be replaced by the Officers.
7. Laptops stolen at workshops and were not secured shall be replaced by the officers.
8. Damaged laptops shall be replaced by the officer who collected them.

Guidelines:

1. All procured laptops shall be checked by the ICT Unit for compliance to the specifications before installation.
2. Laptops shall always be locked with a laptop lock.

3.0 SHARING OF RESOURCES PROJECTORS, PRINTERS AND SCANNERS STANDARDS AND GUIDELINES

The Standards and Guidelines outlined in this document govern these resources and how they shall be shared in the Ministry.

1. Projectors, printers and scanners shall be shared by users in the Ministry.
2. All requests to move these shared resources from allocated stations shall be made through the ICT Unit.
3. All installation and configuration of these resources shall be undertaken by the ICT Unit.
4. All requests to move these shared resources offsite shall be approved by ICT Unit before the items are released.

Guidelines:

1. Projectors, printers and scanners shall be configured by the ICT Unit in a manner that shall allow multiple users access the limited resources with ease.

4.0 DISASTER RECOVERY STANDARDS AND GUIDELINES

The ICT unit disaster recovery process will constitute testing of the backup which shall be done quarterly.

4.1 Server Backup

This guideline covers backing up of all data and files for MoH and its Institutions.

1. Mail servers shall be backed up on a daily basis
2. MoH managed financial servers shall be backed up on a daily basis
3. File servers will be backed up on a daily basis
4. All MoH managed health information systems shall be backed up weekly
5. Domain Controller, Antivirus and all other servers will be backed up monthly

4.2 Backup Standards and Guidelines

Guidelines:

1. All users shall store documents in the documents folder. ICT will not be responsible for loss of data not on the prescribed location.
2. Computer users shall be responsible for ensuring that the data stored on their local machines is backed up to external media as required by the owner.

5.0 INFORMATION AND COMMUNICATION TECHNOLOGY HELP DESK

The ICT Help Desk shall provide the users with an entry point for handling all aspects of contact with ICT services. The purpose of the Help Desk is to troubleshoot problems, provide guidance about resources such as computers and all other related ICT equipment.

Guidelines:

1. Users shall contact the helpdesk via email or telephone to lodge in a complaint
2. The help desk shall raise a maintenance requisition log which the ICT Unit shall respond to on first come first out basis dependent on level of priority and duration to complete task.

6.0 EQUIPMENT SPECIFICATIONS STANDARDS AND GUIDELINES

Guidelines for ICT equipment specifications have been compiled to provide the Ministry with systematic mechanisms for dealing with hardware donations and acquisitions.

a. In view of the current ICT environment, the following hardware devices shall typically be required:

i. PCs: Fat-clients configurations shall be used for all user operations while thin-clients configurations shall be acceptable for use in training schools.

ii. Printers: Monochrome printers shall be used with colour as an option. Colour printing is a higher-cost option, and shall not be recommended.

iii. Servers: Servers and workstations shall be used to share resources.

iv. Peripherals:

- Data projectors / interactive whiteboards (IWB).

- Scanners – with automatic document feeder (ADF)
- Digital Cameras
- External Drives

b. Software to be used in the Ministry as defined in the specifications in appendix A.

i. Operating systems.

ii. Utility programs.

iii. Applications.

c. Refurbished / donated equipment

The specifications below provide guidance for the entry-level standard for the year 2014 - 2016

i. Minimum 2.6GHz CPU.

ii. Minimum 4GB RAM.

iii. Minimum 500GB hard disk.

iv. Integrated Graphics Controller.

v. Minimum 19" LCD monitor.

vi. Maintenance and support agreement of 2-3 year on-site warranty, shall accompany donations to ensure the availability of the system.

d. Donated equipment - It is recommended that any donated equipment shall adhere to the minimum ICT specification stated in the appendix A**.**

7.0 SECURITY STANDARDS AND GUIDELINES

The purpose of the security standard is to protect the Ministry and user resources. Levels of security are at application, system and network.

Passwords in the wrong hands have implications to breach confidentiality**.** Passwords are an important aspect of security in a computer environment. They are regarded as the front line of protection for user accounts and access to network devices. A poorly chosen password may result in the compromise of the ministry's entire corporate network. As such, all Ministry employees are responsible for taking the appropriate steps to secure their passwords.

Guidelines:

1. The ICT Unit shall only support passwords that are managed on the domain for its users. In cases of installation without domains only Ministry equipment shall be supported.
2. MoH equipment that is not on the domain shall adhere to security standards and guidelines as defined by the ministry.
3. No users shall be allowed to share a password with another. The purpose of this is to secure their domain account and login which is attached to their corporate email and possibly sensitive documents.
4. Passwords shall not be displayed on walls or notice boards.

7.1 Physical Security Standards and Guidelines

The purpose is to ensure that ICT equipment is physically secured and network resources protected.

Guidelines:

1. Access to the server room or offices that act as server rooms shall be restricted and regulated to only authorised persons. A log in procedure shall be enforced to control access by authorised personnel.
2. All MoH laptops shall be procured with cable locks and users shall be required to use them at all times.
3. All MoH ICT infrastructure connected to the network shall be physically secured.
4. All users shall lock their device on the network upon leaving their device unattended to.

5. All users shall shutdown/power off their devices on the network at knocking off time

7.2 Network Security Standards and Guidelines

This standard is intended to mitigate the risks and losses associated with security threats to the Ministry Network.

Guidelines:

1. The user agrees to behave in an ethical manner and shall be responsible for his or her own actions. Under the ICT Act, any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program or data is guilty of a felony. Refer to appendix B – User Acceptance.

2. The ICT unit shall not allow any unauthorised device that is unknown on its inventory to connect to the network to access resources. This is to protect against external threats such as malware, hacking and also to preserve internet bandwidth.

3. The user understands that the network is a shared resource and shall not intentionally take actions that interfere with the operation, integrity or security of the network.

4. The user shall not provide access to third parties without the approval of the ICT Unit.

5. The user understands that any fraud to network traffic and files shall be subject to search under Court order. In addition, system administrators may monitor network traffic or access user files as required to protect the integrity of the computer network. (Refer to Section 26b)

6. The user understands that access to the network shall be temporarily suspended during maintenance and that the ICT Unit shall not be liable for damages due to a failure of some network service or due to a breach of security. Prior notice shall be given to users when there is maintenance and it should be scheduled.

7. The user understands that misuse of networking resources may result in the loss of privileges. Additionally, misuse can be prosecuted under applicable statutes. The user may be held accountable for his/her conduct under any applicable Government policies, procedures, or agreements. Complaints alleging misuse of network resources shall be directed to those responsible for taking appropriate disciplinary action.

8. Permission to access documents of an absentee user shall be granted by the supervising officer. Refer to appendix C – Access to Documents

a. Network Connectivity

Guidelines:

1. Anyone wishing to attach a new piece of data equipment to the network shall contact the ICT Unit prior to doing so and follow the appropriate procedures.

2. Any equipment attached to the network shall be bound by these guidelines and its owner is subject to the BYOD and user acceptance guidelines.

b. Service Provision

Guidelines:

1. Providers of network services such as file/print, VPN, proxy, Web Services shall adhere to the standards.

2. Network services provided shall not interfere with existing services on the network.

c. Monitoring, scanning and blocking

Guidelines:

1. Network traffic generated by users of computer systems on the network shall be monitored.

2. Network devices that are identified as being vulnerable to or having suffered a security breach shall be removed from the network at the discretion of the ICT unit and users notified until the problem is resolved.

3. Network services having vulnerabilities that are known to pose a significant threat to MoH network security shall be blocked from the network at the discretion of ICT.

4. Any device or equipment that interferes with the MoH wired or wireless network, including, but not limited to, devices creating radio interference and unauthorised wireless access points, shall be removed from the network at the discretion of the ICT unit unless it has consented in advance to such interference. ICT shall notify the user responsible but if they are unable to make contact quickly, the violating device shall be removed without notice. (Refer to 7.2.2)

d. Remote Access

Guideline:

In order to preserve the safety and integrity of the data communications network, MoH authorised users shall use encrypted connections when connecting remotely to the network as stated in the Bring Your Own Device section of 12.0.

8.0 MEDIA COPYRIGHT STANDARDS AND GUIDELINES

The violation of the Zambian Copyright Law is a serious concern when videotape, CD or DVD duplication of any materials is performed without consent. Any violation of Copyright Law shall potentially put the Ministry's ICT services, its staff, and any user liable to prosecution according to the Copyright Act Cap 400 of the laws of Zambia. This standard shall therefore help the Ministry to impose restrictions regarding what materials shall be legally duplicated.

Guidelines:

1. In order to copy any recorded file on media when one is not the producer or author, one shall have received explicit written consent from the copyright holder for that program.
2. No copy of any material shall be made using the ministry's facilities without explicit written permission or license from the copyright holder.
3. Copyright holders reserve the right to provide or deny permission for duplication.

9.0 HUMAN RESOURCE INFORMATION SYSTEM STANDARDS AND GUIDELINES

The Human Resource Information System (HRIS) is a software or online solution for data entry, data tracking and data information needs of the Human Resources, payroll, management and accounting functions within the Ministry.

1. The Directorate of Human Resource and Administration shall ensure that the data entered in the system is accurate and correct
2. The HRIS shall not be installed on Laptops to safeguard confidentiality of the information in the event of loss of the device.

Guidelines:

1. All HRIS users shall be given orientation on the use of the system.
2. All HRIS users shall safeguard their passwords.
3. All requests for user manuals shall be made available through HRA.
4. Suggestions of new user requirements shall be submitted to the Directorate of Human Resource and Administration.

10.0 TELE-HEALTH STANDARDS AND GUIDELINES

The standards provided cover the fundamental requirements to be followed in providing remote medical services, interactive patient encounters, and other electronic communications between patients and practitioners, for the purposes of health care delivery. These standards apply to individual practitioners, group practices, health care systems, and other providers of health related services.

Guidelines:

1. All institutions providing Tele-Health services are mandated to have policies that comply with MoH guidelines for managing electronic health records.
2. All institutions shall ensure compliance with Health Professional Council of Zambia on relevant legislation, regulations, and accreditation requirements for supporting patient/client decision-making and consent, including protection of patient health information.

11.0 COMPUTER ANTI-VIRUS STANDARDS AND GUIDELINES

The ICT Unit shall provide a computing network that is computer virus-free. The standards and guidelines provide instructions on measures that shall be taken by MoH employees to help achieve effective virus prevention and detection.

Guidelines

1. All computers attached to the MoH network shall run standard and supported anti-virus software. This anti-virus software shall be active at all times and shall be configured to perform on-access real-time checks on all executable files and scheduled virus checks at pre-set intervals. The virus definition files shall be kept up to date at all times.

2. The current MoH standard anti-virus for Microsoft Windows Operating System clients and servers is based on Kaspersky anti-virus solution. All MoH devices shall conform to this solution unless with permission from the ICT unit.

3. Any activity intended to create and/or distribute malicious programs onto the MoH network(s) such as viruses, worms, Trojan horses, e-mail bombs shall be prohibited.

4. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she shall immediately report such an incident to the ICT Unit.

5. All employees shall scan all external media at each connection. The media can only be used on completion of scan.

6. The ICT Unit shall only support the standard licensed anti-virus software provided by MoH .

7. Users shall never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

8. Users shall never open files or macros attached to an e-mail from a known source even a co-worker if you were not expecting a specific attachment from that source.

9. Users shall be suspicious of e-mail messages containing links to unknown web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

12.0 BRING YOUR OWN DEVICE - STANDARDS AND GUIDELINES

This standard provides rules of behaviour for the use of personally-owned smart phones and/or tablets by MoH employees herein referred to as users, to access MoH network resources. Access to and continued use of network services is granted on condition that each user reads, signs, respects, and follows the MoH User Acceptance concerning the use of these devices and services.

Current devices recommended for use for BYOD

- Android Smart Phones & Tablets
- Blackberry Smart Phones & Playbook
- iPhones & iPads
- Laptop

1. Expectation of Privacy: MoH shall respect the privacy of your personal device and shall only request access to the device by technicians to implement security controls.
2. While access to the personal device itself is restricted, Government Policy on rules of behaviour regarding the use/access of government e-mail and other government system/service shall remain in effect.
3. In situations where there are questions related to compliance with the security requirements, the user may opt out of the BYOD programme declining to give the device to ICT for compliance verification.

Guidelines for all BYODs accessing MoH network services:

1. A user shall not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorised access can adversely affect the privacy or welfare of an individual, agency or financial operations.
2. A user shall password protect the device.
3. A user agrees that the device shall not be shared with other individuals or family members, due to the business use of the device such as potential access to government e-mail.
4. A user agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments. ICT shall provide instructions for identifying and removing these unintended file downloads. Users shall follow the principle, "When in doubt, delete it out."
5. If the device is lost or stolen, the user shall notify the ICT Unit within one hour, or as soon as possible.
6. A user shall comply with all MoH password guidelines, including use of strong passwords.
7. A user shall maintain up to date anti-virus protection on their device.
8. A user shall not download/transfer sensitive MoH business data/documents to any non-MoH device.
9. A user shall only use MoH approved and configured Virtual Private Network client software to access MoH's VPN.

13.0 mHealth STANDARDS AND GUIDELINES

The Ministry of Health with support from cooperating partners has been championing the use of mobile technology to help improve the delivery of timely quality health care.

Guidelines:

1. MoH ICT shall be involved in all mHealth initiatives from inception so that they provide guidance and direction.
2. The Ministry reserves the right to reject any mHealth initiatives that shall pose a risk to the security of health information systems.
3. All partners with interest in mHealth shall be part of the mHealth Technical Working Group. This shall enable all stakeholders to be up to date with developments in the sector and share resources and experiences so that the Ministry's ultimate goal of systems integration is achieved.
4. Cooperating Partners shall not introduce and run mHealth programmes in isolation.
5. Duplicate work being undertaken by other partners shall not be allowed, but synergies shall be encouraged.

14.0 MOVEMENT OF ICT EQUIPMENT STANDARDS AND GUIDELINES

The Ministry of Health has faced challenges in tracking the movement of ICT equipment. When officers are transferred, not all ICT equipment is surrendered. This has led to loss of equipment, there is need to clearly state the steps to follow when officers are leaving or want to move equipment from one location to another.

Guidelines:

1. HRA shall inform ICT when an officer is about to be transferred at least two weeks before the officer leaves so that ICT can ensure that they issue the officer a form to confirm that they have handed over all ICT equipment that they were using.
2. When officers are going out on official duty, they shall inform ICT at least two days before they leave if they are in need of ICT assistance.
3. All ICT equipment moved from one office to another shall be done under the supervision of ICT and Administration. The ICT unit reserves the right to lock down equipment as per inventory record and the user shall comply with this.
4. No ICT equipment shall be transferred from one officer to another without the consent of ICT. Officers must fill in an appropriate equipment transfer form in quadruplicate to ICT, Stores, Personal file and recipient.

15.0 PROCUREMENT AND DISPOSAL OF ICT EQUIPMENT STANDARDS AND GUIDELINES

The goal of the Ministry is to maintain standardised ICT equipment in the country. This standard is intended to help in simplifying ICT procurements and disposal of all outdated and none functional equipment as well as prevent the wastage of ICT equipment that can be potentially useful.

Guidelines:

1. All ICT equipment specifications shall be dated indicating the requesting unit or department, the quantity and shall be signed by ICT for specific procurements and cannot be reused in another procurement.
2. All programme managers shall inform ICT of their ICT equipment procurement plans at the end of January of every year. ICT shall provide signed and dated specifications for the Procurement and Supplies Unit to ensure that suppliers do not supply wrong equipment. When the equipment is supplied, the Stores Unit shall hand over the equipment to ICT for inspection. If the equipment meets all the specifications then ICT shall inform Stores, install and configure the equipment for use. If the equipment does not meet the requirements, then ICT shall reject the equipment and inform procurement and stores why they have rejected the equipment.

3. All ICT equipment that does NOT meet the specifications and has not been inspected by ICT shall not be configured and shall NOT be granted access to any technical support or resources such as network or internet connectivity.
4. All external hard drives shall be handed over to ICT when officers are transferred to another Ministry. Users shall only be allowed to move with equipment in situations where they are promoted or change positions in the same Directorate/Unit.

Disposal

The disposal of ICT resources shall be done in accordance with government guidelines and procedures as stipulated by the Ministry of Transport, Works, Supply and Communications.

1. All ICT equipment shall have a minimum lifespan as set in the table below. Equipment shall be assessed before it is considered obsolete. The ICT unit shall maintain an updated inventory of all ICT equipment. The inventory records shall include the date and cost the equipment was procured, the officer using the equipment and the condition.

   Table: Listing minimum lifespan of ICT equipment

No.	Equipment	Minimum Lifespan
1	Laptops	5 years
2	Desktops	6 years
3	Printers	7 years
4	Scanners	9 years
5	Projectors	6 years
6	UPSs	3 years
7	Wireless Access Points	7 years
8	Network switches	10 years
9	Routers	10 years

2. When ICT equipment becomes faulty or damaged, it shall be inspected by the ICT unit. The ICT unit shall verify and state whether the equipment can be repaired or not. For equipment that cannot be repaired, the ICT unit shall ensure that any information retrieved is backed up or transferred. All reusable hard drives and functional components shall be removed from the computers that are irreparable as spares.
3. The faulty or damaged equipment shall be surrendered to the stores unit.
4. All ICT equipment shall have a service warranty of minimum one (01) year

16.0 WEBSITE STANDARDS AND GUIDELINES

The goal of the Ministry of Health is to maintain a user friendly up to date and relevant website. The Ministry shall also maintain web presence through various social media platforms. The website shall provide the Ministry an opportunity to get public feedback on the delivery of health services and whether the Ministry is meeting its intended goals and objectives.

Guidelines:

1. The website email addresses and social media links shall be included on all official publications, productions and letter headed paper.
2. The website shall enhance the Ministry's corporate profile and presence on the Internet by providing informative, accurate and verified information.
3. Queries received from the website shall be responded to within 48 hours through the official email addresses; info@moh.gov.zm
4. The social media platform shall be updated daily. The updates shall be approved by the Directorate of Technical Support Services.
5. All social media queries and feedback requests shall be responded to within 48 hours.
6. All official press statements and releases by the Ministry of Health shall be posted on the website and various social media platform after release.
7. All tender documents shall be uploaded on the website immediately after approval by the relevant offices and shall be maintained on the website until they expire.
8. Confidential information or documents shall not be published on the website or any social media platforms.
9. The official Ministry of Health logo shall be displayed on all web pages.
10. All MoH institutions with websites shall use subdomains under the moh.gov.zm domain. This shall be done in consultation with MoH ICT Unit at HQ.
11. All MoH institutions with websites shall form a website team that will meet to approve content.

17.0 SMARTCARE HEALTH INFORMATION SYSTEM STANDARDS AND GUIDELINES

SmartCare is the approved patient level health care information system, in accordance to the circular of 5th April, 2006 from the office of the Permanent Secretary.

Guidelines:

1. Patient data shall be entered into SmartCare daily in all facilities where it is deployed.
2. All patients entered into the SmartCare System shall be issued with care cards – smartcards.
3. The HIA2 report for the District Health Information System shall be produced from SmartCare for each facility to improve efficiency and minimise data errors.
4. Health facilities shall merge databases within the facility where systems are standalone every week
5. The health facilities shall send a complete database to the district on or before the 7th of the following month. This is the responsibility of the health facility in charge to ensure that this is done.
6. The district shall merge and submit the district database to the province on or before the 21st of the month when the complete database was received.
7. The 2nd and 3rd level hospitals shall submit merged databases to the provincial office on or before the 21st of the following month.
8. The Provincial office shall merge and submit the databases to the national office on or before 28th of the following month.

18.0 TELEPHONE ACCEPTABLE USE STANDARDS GUIDELINES

The Ministry of Health provides telephone system and telecommunication services for use by employees to conduct government business.

At a minimum, all telephone switchboard systems used by the ministry shall comprise the following features to enable efficient use of the telephone system resources:

1. Voice over Internet protocol (VoIP)
2. Pass code dialling
3. Voice mail feature
4. Call forwarding feature
5. Call recording
6. Least cost routing

Optional:

7. Pre-Paid services

Guidelines

The following shall be the acceptable use guidelines in the usage of telephone system resources.

a. The ministry shall provide pre-paid telephone service or pass code dialing or both in order to regulate telephone resource usage.
b. Calls to staff within the VoIP network shall be to their extension numbers and not to landline or mobile numbers to minimize cost.
c. All telephone calls or faxes made on ministry resources shall be accounted for in a register, where pass code dialing is unavailable.
d. The ministry shall permit minimum use of the telephone system for personal, appropriate and reasonable use within set guidelines.
e. All PABX systems shall be network ready.

1. Personal responsibility
   By accepting responsibility for pre-paid phone cards or establishing your account pass code to access the ministry's telephone system and resources, members of staff agree to adhere to this document. They also agree to report any misuse to the Human Resources and Administration department.

   Users shall bear in mind that telephone calls shall be recorded from time to time and shall be used during disciplinary hearings or litigation shall the need arise.

2. Purpose and Use
   The ministry shall provide access to its telephone systems primarily for government business purposes only.

3. Inappropriate activity

   The Ministry regards the following activities on the telephone network to be inappropriate.

   a. Engaging in cyber bullying in any of its forms.
   b. Using the Ministry's telephone system to seek or make inappropriate offensive, vulgar, suggestive, obscene, abusive, harassing, threatening, defamatory (harming another person's reputation by lies), disparaging or misleading language or materials.
   c. Making ethnic, sexual-preference or gender-related slurs or jokes

d. Revealing personal information, such as the home address, telephone number or financial data of another person, or yourself (the security of this information cannot be guaranteed).
e. Engaging in illegal activities, or encouraging others to do so.
f. Using another employee's pass code to make telephone calls in order to evade accountability
g. Engaging in private commercial activity whether on telephone or fax.

4. Confidential Information
Unless authorised to do so, employees shall be prohibited from using the telephone system to convey confidential information to outside parties. If in doubt, reference shall be made to the Civil Service Confidentiality Clause document signed at the beginning of employment and Personal Responsibility Clause.

5. Personal use of telephones
The ministry is aware that there may be occasions when employees shall need to use the telephone system for personal communication. Personal use of these shall be kept to a minimum and shall be considered reasonable providing that it does not impact on the ministry's duties and shall not contravene these guidelines.

Employees are not allowed to use the ministry's telephone systems and related resources to operate a business, or solicit money for personal gain.

6. Acknowledgement
All employees shall be aware that failure to comply with this document shall result in the withdrawal of services and/or result in disciplinary action up to and including dismissal

19.0 EMAIL ETIQUETTE STANDARDS AND GUIDELINES

The purpose of email is to get the message across clearly to the people who need information you are providing. Ministry staff shall follow the standards and Guidelines on email etiquette in order to assist in communicating effectively:

Guidelines:

1. Staff shall ensure that they are addressing their mail to the correct person or group.
2. When a member of staff receives wrong email, the recipient shall reply saying the email is not meant for him/her.
3. Staff shall only send the email "to" the person they are addressing directly and "cc" to indirectly addressed persons.
4. Staff shall be encouraged to create email lists if they regularly send emails to a group of persons.

5. Staff shall use “reply to all” if everyone they are replying to is interested in their response.
6. Staff shall include a short “subject” line in their email.
7. Staff shall use attachments with caution. Only relevant attachments shall be allowed.
8. Staff shall always be cautious before they forward any email and they shall explain to the recipient why they are sending it.
9. Staff shall never respond to spam. Delete the message instead as it may contain viruses or spyware.

20.0 IFMIS STANDARDS AND GUIDELINES

The Integrated Financial Management and Information Systems (IFMIS) . This is a SAP financial management application that is centralised and meant handle all financial management functions into one suite of applications. It is an ICT-based budgeting and accounting system designed to assist Government entities to plan budget requests, spend their budgets, manage and report on their financial activities, and deliver services to the public more efficiently, effectively and economically.

Guidelines:

Users of the Integrated Financial Management Information System in the Ministry shall follow the standards and Guidelines outlined below:

1. IFMIS users shall be oriented in the use of the system.
2. IFMIS users shall have correct username/ID and password in order to have access into the system.
3. If users encounter technical problems while working with the system, they shall contact the ICT Help Desk for intervention.
4. IFMIS users shall not share their username/ID and password with other persons.
5. The system shall keep a log of all users of the system from login to logout.
6. Users shall not attempt to circumvent or subvert the system for security reasons.

21.0 LABORATORY INFORMATION MANAGEMENT SYSTEM STANDARDS AND GUIDELINES

Laboratory Information Management System (LIMS), sometimes referred to as a Laboratory Information System (LIS) or Laboratory Information Management System (LIMS), is a software based laboratory and information management system that offers a set of key features that support modern laboratory operations. These key features include but not limited to - specimen management, manual and automated testing of specimens, stock management, traceability for test specimens, production of all sorts of reports for decision making and biomedical research, planning purposes and for the improvement of patient care.

Users of the Laboratory Information System in the Ministry shall follow the guidelines outlined below:

Guidelines:

1. Selected laboratory and ICT personnel shall be trained as super users.
2. Laboratory Staff and other support personnel shall be oriented to use the system by super users and the software vendor
3. Staff shall have correct username/ID and password for the system in order to have access into the system.
4. If users encounter technical problems while working with the system, they shall contact the ICT help desk for the quick intervention.
5. Staff shall not share their username/ID and password with other persons.
6. The system shall keep a log of all users of the system from login to logout.
7. Users shall not attempt to circumvent or subvert the system for security reasons
8. The system shall be backed up periodically.
9. Passwords shall be changed periodically.
10. Users accounts shall be deactivated when inactive for prolonged periods
11. All ICT technical problems shall be reported to the ICT Office
12. All LIS Lab Technical Issues shall be reported to the assigned Super user
13. The computer with the LIS system shall log off a user after 5 minutes of idle time
14. Users shall not plug any USB device into the LIS PC
15. Staff shall not be allowed to share patients data with unauthorized persons and confidentiality shall be upheld.

22.0 LOGISTICS INFORMATION SYSTEM STANDARDS AND GUIDELINES

Users of the Logistics information system(s) in the Ministry shall follow the standards and guidelines outlined below:

Guidelines:

1. Staff shall be oriented to use the system.
2. Staff shall have correct username/ID and password for the system in order to have access into the system.
3. When users encounter technical problems while working with the system, they shall contact the ICT help desk for the quick intervention.
4. Staff shall not share their username/ID and password with other persons.
5. The system shall keep a log of all users of the system from login to logout.
6. Users shall not attempt to circumvent or subvert the system for security reasons
7. The system shall be backed up periodically.
8. The system shall have a preventive maintenance plan for both the hardware and software components.
9. The system shall produce audit trail reports.

23.0 MICROSOFT DYNAMICS NAVISION SYSTEM

Microsoft Dynamics NAV is an enterprise resource planning (ERP) software product from Microsoft. The product is part of the Microsoft Dynamics family, and intended to assist with finance, manufacturing, customer relationship management, supply chains, analytics and electronic commerce for small and medium-sized enterprises.

Users of the Navision System in the Ministry shall follow the standards and guidelines outlined below:

Guidelines:

1. They shall be oriented to use the system.
2. They shall have correct username/ID and password for the system in order to have access into the system.
3. When users encounter technical problems while working with the system, they shall contact the ICT help desk for the quick intervention.
4. They shall not share their username/ID and password with other persons.
5. The system shall keep a log of all users of the system from login to logout.
6. Users shall not attempt to circumvent or subvert the system for security reasons.

7. The system shall have a preventive maintenance plan for both the hardware and software components.
8. The system shall produce audit trail reports.

24.0 SOFTWARE DEVELOPMENT STANDARDS AND GUIDELINES

Software development refers to the activity of computer programming which is the process of writing and maintaining source code.

All requests for software development shall be initiated by the users themselves. They shall be encouraged to take up an initiative in requesting for new systems/system modifications and also for them to describe specific results or requirements to be obtained. The standards and Guidelines outlined in this document govern any requests for any development of software in the Ministry.

Guidelines:

1. Request for software development shall be initiated by Users to ICT Unit through the office of the Permanent Secretary explaining the business area in terms of the following;
   - the problem to be solved;
   - the results expected or objectives that are to be achieved;

2. The software development project shall be reviewed for correctness by the ICT Unit who shall amend any technical information required in considering the project.

3. The ICT Unit shall send the user a copy of the system proposal as revised by the ICT Unit, the recommendations for approval or disapproval, the priority assigned to the project, the expected date for beginning work on the preliminary design, and the support expected from the user department.

4. All software development projects shall be reviewed by the users and the ICT Unit in order to be certain that the software and its results shall be consistent with the organisation's objectives.

5. All the software implemented shall be given different version numbers.

6. All software implemented shall have documentation on the hardware requirements and user manual.

25.0 SOFTWARE INSTALLATION REQUEST STANDARDS AND GUIDELINES

Installation of a computer program is the act of making the program ready for execution. Because the process varies for each program and each computer, programs often come with an installation CD.

The ICT unit maintains the hardware and software in the Ministry of health. The standards and Guidelines outlined in this document govern any requests for new software in the Ministry.

Guidelines:

1. All requests shall be made at least one week prior to the date needed for use.
2. All requests for new software installations shall be made through the ICT Unit. The ICT Unit shall prepare a Software Installation Request Form and the supporting materials outlined on the form and in this document.
3. All requests shall be given a Service Request number (SR#).
4. To receive a service request number, the ICT shall have:
    - Copies of the installation media;
    - Copies of the installation instructions;
    - Copies of the license key and license terms.

5. All requests shall be approved by ICT Unit before being assigned to an officer
6. The request shall be denied if:
    - An insufficient number of licenses is supplied
    - The software is known to interfere with other applications on the MoH network
7. Obtain the Installation Request form from the ICT Unit
8. The member of staff requesting the software installation shall sign off on the installation affirming the functionality of the software.

26.0 INTERNET USE STANDARDS AND GUIDELINES

The standards and guidelines outlined in this document govern use of the Internet by employees of the Ministry. Employees shall be permitted and encouraged where such use supports the goals and objectives of the Ministry.

Computer, Email and Internet Usage

a. Acceptable use of the Email and Internet by employees includes, but is not limited to:

1. Employees shall use the Internet responsibly and productively. Internet access shall be limited to job-related activities only and personal use is not permitted
2. Job-related activities shall include but not limited to research and educational tasks that may be found via the Internet that would help in an employee's role

3. All Internet data that is composed, transmitted and/or received by the MoH computer systems is considered to belong to MoH and shall be recognised as part of its official data. It is therefore subject to disclosure to appropriate third parties for legal and other reasons
4. The equipment, services and technology used to access the Internet are the property of MoH and the Ministry shall reserve the right to monitor Internet traffic.
5. Emails sent via the Ministry's corporate email system shall not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.
6. All sites and downloads shall be monitored and/or blocked by MoH if they are deemed to be harmful and/or not productive to business

b. Unacceptable use of Email and the Internet by employees includes, but is not limited to:

1. Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via MoH email service.
2. Using computers to perpetrate any form of fraud, and/or software, film or music piracy
3. Stealing, using, or disclosing someone else's password
4. Sharing of passwords including network passphrases
5. Downloading, copying or pirating software and electronic files that are copyrighted or without authorisation
6. Sharing confidential material, trade secrets, or proprietary information outside of the organisation
7. Hacking
8. Sending or posting information that is defamatory to the Ministry, its services, colleagues and/or partners
9. Introducing malicious software onto the company network and/or jeopardising the security of the organisation's electronic communications systems.
10. Sending or posting chain letters, solicitations, or advertisements that are not related to business purposes or activities.
11. Passing of personal views as representing those of MoH
12. Accessing, downloading or viewing inappropriate or illegal material

27.0 NAMING CONVENTIONS STANDARDS AND GUIDELINES

The intent of a naming convention is to allow useful information to be deduced from the names based on regularities. Ministry of Health shall use a scalable, unique and easy to remember naming conversion for its network resources.

- Computer names shall consist of the short code identifying the department/unit and part of the user name for accounts computers.
- Laptop names shall consist of the short code identifying the department and part of the user name followed by the letter L denoting laptop.
- User names shall consist of the first letter of the users first name followed by the last name.
- Corporate Email addresses shall have the form of username@moh.gov.zm. Each email address shall also have an alias email address of FirstName.LastName@moh.gov.zm
- Folders- ICT shall provide a central file storage system through a file server where a LAN exists. The file server shall be the primary storage location for work-related files. The following guidelines shall help Ministry of Health staff to classify appropriately electronic files and folders and to use properly the storage area available on the shared drive.

Guidelines:

1. All documents shall be gathered in one folder concerning a specific activity or subject
2. All folders shall be structured hierarchically and related to a programme or activity
3. Avoid duplications of folders
4. Classify all documents in correct versions on folders
5. Do not use last names or first names for folders
6. Avoid abbreviations except official acronyms
7. Leave space between the folder names for example: malaria indicators
8. Avoid punctuation signs like : _/!*) for folder names
9. Users shall save all official documents on specified folders

28.0 CCTV AND ACCESS CONTROL STANDARDS AND GUIDELINES

Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors for surveillance in areas that may need monitoring in the ministry of health or its institutions.

The basic principles and recommendations shall, in most cases, be applied to any system using CCTV cameras and video recorders. This document addresses both analog and digital video systems. The intent of these recommendations and guidelines is to optimise image quality to facilitate the identification of people and objects depicted therein.

Guidelines:

1. All CCTV schemes that process data about a known person are obliged to conform to certain legislation, most importantly the ZICTA Act, ECT Act and the Human Rights Act. They give recommendations for the operation and management of CCTV and assists owners of CCTV schemes to follow best practices in obtaining reliable information that shall be used as evidence.
2. All areas monitored by CCTV cameras shall have a poster clearly warning members of the public about their availability.
3. Recordings that depict criminal activity shall be preserved in a manner that permits law enforcement officials to recover the original images with a documented chain of custody
4. The Ministry shall establish and follow a program of regular system maintenance.
5. CCTV systems shall include the following components, at a minimum: a camera or cameras, moveable and/or fixed; a monitor; and a recording device, including the means by which the recording may be extracted from the device. Consideration shall also be given to any need for recording audio with the video from one or more cameras and any legal problems unique to audio recording.

29.0 CLOUD COMPUTING STANDARDS AND GUIDELINES

The purpose of these general guidelines is to ensure that the contracts entered in with cloud computing service providers and their associated Service Level Agreement (SLA) have appropriate provisions for security and privacy. In particular, the SLA shall help maintain legal protections for privacy relating to data stored on the provider's systems. The Ministry shall also ensure appropriate integration of the cloud computing services with their own systems. The cloud computing provider should conform to the following standards and guidelines.

Guidelines:

1. **Ensure effective governance, risk and compliance processes exist**

   The Ministry shall ensure that a cloud computing provider complies with MoH established security and compliance policies and procedures.

2. **Audit operational & business processes**
   The cloud provider shall furnish the Ministry with a report of the cloud provider's operations by independent auditors. Unfettered access to essential audit information shall be a key consideration of contracts and SLA terms with any cloud provider. As part of any terms, cloud providers shall offer timely access to and self management of audit event, log and report information relevant to Ministry's specific data or applications.

3. **Manage People, Roles and Identities**
   The Ministry shall ensure that a cloud provider has processes and functionality that governs who has access to the consumer's data and applications. This ensures access to their cloud environment is controlled and managed.
4. **Ensure Proper Protection of Data and Information**
   Security considerations shall apply both to data at rest (held on some form of storage system) and also to data in motion (being transferred over some form of communication link).

   Data In Motion – Data in motion shall be protected by encryption through the use of secure data transfer protocols like https.
   Data At Rest – Data at rest shall be protected from theft or unauthorised disclosure, tempering, unauthorised modification, loss and unavailability.

5. **Enforce Privacy Policies**

   Privacy issues shall be adequately addressed in the cloud contract and SLA including adhering to laws and regulations, relating to the acquisition, storage and use of Personally Identifiable Information (PII). If not, the Ministry shall consider alternate means of achieving its goals including seeking a different provider, or not putting sensitive data into the cloud computing environment.

6. **Assess The Security Provisions For Cloud Applications**

   Clearly defined security policies and processes are critical to ensure that cloud applications are enabling the functions of the Ministry rather than introducing additional risk.

7. **Ensure Cloud Networks And Connections Are Secure**

   A cloud service provider shall allow legitimate network traffic and drop malicious network traffic.

   External Networks – The cloud provider shall put in certain external network perimeter safety measures. These shall include traffic screening, intrusion detection/prevention, logging and notification.

   Internal Networks – The cloud provider's internal network controls shall be evaluated with respect to the Ministry's requirements and any existing security policies the consumer may have. The internal network controls that shall be considered include. Protection of clients from one another in a multi-tenant set-up, protection measures of the provider's network and monitoring for intrusion attempts.

8. **Evaluate Security Controls On Physical Infrastructure And Facilities**

   The cloud provider shall provide audit and assessment reports, demonstrating compliance to such security standards as ISO 27002.

   The cloud provider shall apply security controls to the physical infrastructure and facilities. These include:

   - **Physical Infrastructure and facilities shall be held in secure areas**. A physical security perimeter shall be in place to prevent unauthorised access, allied to physical entry controls to ensure that only authorised personnel have access to areas containing sensitive infrastructure. Appropriate physical security shall be in place for all offices/rooms and facilities which contain physical infrastructure relevant to the provision of cloud services.
   - **Protection against external and environmental threats**. Protection shall be provided against things like fire, floods, earthquakes, civil unrest or other potential threats which could disrupt cloud services.
   - **Control of personnel working in secure areas**. Such controls shall be applied to prevent malicious actions.

- **Equipment security controls.** Shall be in place to prevent loss, theft, damage or compromise of assets.
- **Supporting utilities such as electricity supply, gas supply, and water supply shall have controls in place**. Required to prevent disruption either by failure of service or by malfunction (e.g. water leakage). This may require multiple routes and multiple utility suppliers.
- **Control security of cabling**. In particular power cabling and telecommunications cabling, to prevent accidental or malicious damage.
- **Proper equipment maintenance**. Shall be performed to ensure that services are not disrupted through foreseeable equipment failures.
- **Control of removal of assets.** Required to avoid theft of valuable and sensitive assets.
- **Secure disposal or re-use of equipment**. Particularly any devices which might contain data such as storage media.
- **Human resources security.** Appropriate controls need to be in place for the staff working at the facilities of a cloud provider, including any temporary or contract staff.
- **Backup, Redundancy and Continuity Plans.** The provider shall have appropriate backup of data, redundancy of equipment and continuity plans for handling equipment failure situations.

9. Manage Security Terms In The Cloud SLA

The SLA shall specify security responsibilities and shall include aspects such as the reporting of security breaches. It shall be explicitly documented in the cloud SLA that providers shall notify consumers about the occurrence of any breach of their system, regardless of the parties or data directly impacted. The provider shall include specific pertinent information in the notification, stop the data breach as quickly as possible, restore secure access to the service as soon as possible, apply best-practice forensics in investigating the circumstances and causes of the breach, and make long-term infrastructure changes to correct the root causes of the breach to ensure that it does not recur.

10. Understand The Security Requirements Of The Exit Process

The provider shall ensure that any copies of the data are wiped clean from the provider's environment, wherever they may have been stored i.e. including backup locations as well as online data stores. The exit process shall allow Ministry of Health to retrieve their data in a suitably secure form, backups shall be retained for agreed periods before being eliminated and associated event logs and reporting data shall also be retained until the exit process is complete.

11. Contract and Service Level Agreement

The Ministry shall ensure its cloud hosted applications and data are secured in accordance with its security policies. The contract between Ministry of Health and the provider, along with an associated SLA shall contain all the requirements of the Ministry. If a suitable contract and SLA is not available, the Ministry of Health will not proceed with the use of cloud services.

The Ministry shall only use facilities outside the country where the government Data Centre cannot handle the MoH needs and clearance shall be obtained in writing from MCTWS.

30.0 BIOMETRIC SYSTEM STANDARDS AND GUIDELINES

Biometric System is a technological system that uses information about a person or other biological organism to identify the person. Biometric systems rely on the specific data about unique biological characters in order to work effectively. It uses an automated method for physical access control to buildings and logical access control to ICT systems based on measurable biological - anatomical and physiological behavioural characteristics.

Users of the Biometrical System in the Ministry shall follow the standards and guidelines outlined below:

Guidelines:

1. They shall be oriented to use the system;
2. They shall have quality initial registration and enrolment of information, that is user identification such as fingerprint
3. All users registered for biometric systems shall have access to controlled areas/systems and should use correct identifications

4. The system shall keep a log of all users in the system from login to logout

5. Users shall not in any way tamper with the biometric hardware or software

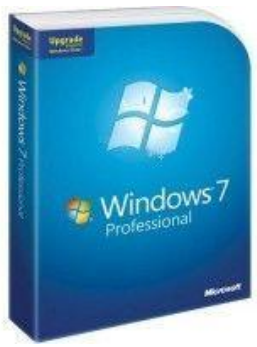
APPENDICES

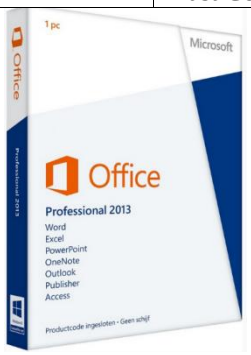
Appendix A Equipment Specifications

Desktop Computer Specifications **DATE**

QUANTITY **(SECTION)**

	Features	**Technical details (Pro 3515)**
1	System Processor/Model	3rd Gen Core i3, Intel 3 i3-3220 / 3.3 GHz
2	Operating System	**Genuine** Microsoft **Windows 7 Professional,** with CD for the genuine installer and tag
3	Standard memory	Minimum: 4 GB, Technology DDR3 SDRAM - Non-ECC
4	Internal drive	Minimum: 500 GB, Serial ATA-600 Serial ATA, Spindle Speed 7200 rpm
5	Optical drive	DVD±RW (±R DL) / DVD-RAM - Serial ATA
6	Graphic card	Intel HD Graphics 2500 Dynamic Video Memory Technology
7	I/O ports	Rear: 4 USB 2.0, 1 RJ-45, 1 VGA, audio in/out, Mic In Front: 2 USB 2.0, audio in/out
8	Audio	Integrated, Stereo, 192 KHz, High Definition Audio
9	Network interface	Integrated, Intel 82579LM, Fast Ethernet, Ethernet, Gigabit Ethernet
10	Display type	**Minimum** 19 inch LCD Display (**with three pin male power connector**)
11	Power	AC 120/230 V (50/60 Hz), 320 Watt, British standard Plug
12	**Warranty**	**1 year**
13	UPS	**Smart UPS 1500**
	***Included**	***Standard British Plug for Systems Unit, Monitor & UPS**
1	Microsoft Office	Preinstalled **Genuine Microsoft Office Professional 2013** with CD\keycard and tag
2	Dust Covers	Dust Covers for monitor and systems unit

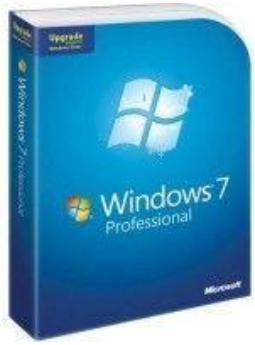


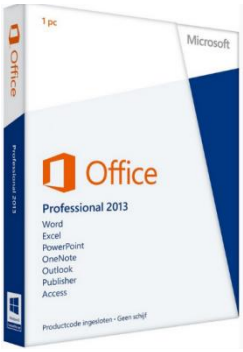


Laptop Computer Specifications **DATE**

QUANTITY **(SECTION)**

	Features	**Technical details**
1	System Processor	**Minimum** Intel Quad Core TM14 i7
2	Operating system installed	**Genuine** Microsoft **Windows 7 Professional edition** with CD for the genuine installer with tag
3	Standard memory	Minimum: 8 GB
4	Internal drive	Minimum: 750GB 5400 rpm SMART SATA II HDD
5	Serial connector	1x9 pin
6	Combo DVDV/CD RW drive	Inbuilt
7	I/O ports	Minimum 3 USB 2.0, 1 RJ-45, 1 VGA, audio in/out
8	Keyboard	US English keyboard (QWERTY)
9	Network interface	10/100/1000 mbps Ethernet
10	Display type	15.6" diagonal LED - backlit HD anti-glare (1366 x 768)
11	Pointing device	Touchpad
12	Blue tooth	Integrated Bluetooth, wireless WiFi link
13	Accessories	AC Adapter with British standard plug, Li-Ion type Battery pack, Type II Card slots
1	Microsoft Office	Preinstalled **Genuine Microsoft Office Professional 2013** with CD\keycard with tag
2	Antivirus Software	**Kaspersky Internet Security 2014** with CD and valid serial
3	Carry Case	**Black/Dark Grey** durable polyester Laptop **back pack**
4		**Laptop Lock (Combination type)**





Printer Computer Specifications **DATE**

QUANTITY **(SECTION)**

Output Type	**LaserJet Enterprise (Duplex/Network)**	**M601dn**
Printer Technology	Laser - Monochrome	
Duty Cycle	Maximum throughput of up to 275,000 pages per month. The recommended monthly print volume is 5,000 to 20,000 pages.	
Print Resolution	The print engine can deliver true 1200 x 1200 dpi. FastRes 1200, ProRes 1200. Actual resolution used depends on job.	
Print Speed	up to 43 ppm - A4 (8.25 in x 11.7 in), up to 45 ppm - Letter A Size (8.5 in x 11 in)	
Multifunction	Printer Only	
Paper Handling	Multipurpose tray for up to 100 sheets of special media in sizes A4, A5, letter, legal etc. Media sizes from 3x4 to 8.5x14 inches.	
Warranty	1 year	
USB	**Yes**	**USB Dot 4 Cable MUST be included (BLACK)**
Platforms Supported	PC	
Ethernet	Yes	
Network Technology	Ethernet 10Base-T/100Base-TX/1000Base-T Gigabit LAN, USB	
Max Media Capacity	1100 sheets	
Output Trays Capacity	500 sheets	
Monthly Duty Cycle	175000 pages 175000 pages	
Features	**Automatic Duplexing**	
Consumables	1 x Toner cartridge (Black) - up to 10000 pages	**MUST be Included**
RAM Installed (Max)	512 MB	
Package Contents	British type Power cord Print cartridge Software and documentation on CD-ROM Start Guide Support flyer Control panel overlay	
Compatibility	Operating Systems: PC: Windows 8, Windows 7, Windows XP, Windows Server 2003/2008	
* **Failure to include USB cable and genuine cartridge will result in printer rejection**		

Scanner Specifications **DATE**

QUANTITY **(SECTION)**

Features:	**Scanjet Pro 3000 s2 (sheetfed scanner) :**
Type Sheetfed scanner	Desktop
Interface Type	USB 2.0
Max Supported Document Size	8.5 in x 34 in
Duty Cycle	1000 scans per day
Scanner Speed Details	20 ppm - 300 dpi (front) / 300 dpi (back), 40 ipm - Duplex - 300 dpi (front) / 300 dpi (back)
Scanner Features	Ultrasonic Multi Feed Detection
Compliant Standards	ISIS, TWAIN, WIA
Supported Media Size Details	ADF - up to 8.5 in x 34 in
Document Feeder Type	Autoload
Cables Included	**1 x USB cable**
Power Device	External power adapter
Voltage Required	AC 120/230 V
Service & Support	1 year warranty
Software included	CD-ROM(s) with software for Windows, HP Smart Document Scan Software, Nuance PaperPort, I.R.I.S. Readiris Pro OCR, NewSoft Presto! BizCard, EMC ISIS/TWAIN drivers
***USB Cable MUST be included**	

Projector Specifications **DATE**

QUANTITY **(SECTION)**

General	System	**Sony VPL-EX7**
	Power Requirements	AC 100 to 240 V, 2.6 to 1.1 A, 50/60 Hz
	Projection System	3LCD panels with Bright Era Technology, 1 lens projection, 40 to 300 screen coverage
	Resolution	High Picture Quality & Brightness (1024 x 768) Extended Graphics Array Resolutions
	Video Compatibility	NTSC, NTSC 4.43, PAL, PAL-M, PAL-N, PAL 60, SECAM
	Projection Lens	1.2 times zoom lens, f=18.53 to 22.18 , F1.65 to 1.93
Size	Dimensions (WxHxD)	314 x 109 x 269 mm
	Mass Approx	2.9 kg
Connectivity	Inputs/Outputs/Signal	15kHz RGB/Component 50/60 Hz
		Progressive Component 50/60 Hz
		DTV (480/60i)
		Signals Video: 575/50i, 480/60p, 575/50p
		Video Input (Composite Video) x 1
		Video Input (S Video) Mini DIN 4 pin x 1
		Input A (RGB/Component) HD D-Sub 15 pin x 1
	Audio	Input x 1
	Remote RS-232C	D-Sub 9-pin (female)
Operation	Audible Noise	29 dB
Optical	Lamp 190 W	Ultra High Pressure Lamp
	Color Light Output	2000 lumens (High lamp mode), 1500 lumens (Standard lamp mode)
	Screen Coverage	40 to 300 inches
	Throwing Distance	40-inch Approx. 1.1 to 1.4 m
In The Box		Remote Control with Batteries
Included		**Soft Carrying Case**
Extras to be Included	1. Roof Mounting 2. 3 Meter Power Cable from Roof Mounting 3. 5 Meter LCD to PC Cable	

Appendix B User Acceptance

MINISTRY OF HEALTH

INFORMATION & COMMUNICATION TECHNOLOGY UNIT

USER ACCEPTANCE FORM

The following must be completed by the person making the request and signed by their supervisor before ICT can assign any equipment.

i. I have read the Ministry of Health's Electronic Mail Acceptable Use Standards and fully understand the terms and conditions and agree to abide by them.

ii. I understand that the ministry's security systems may record for management use all e-mail activity undertaken by me including any material transmitted or received.

iii. I understand that violation of these guidelines may lead to disciplinary action and could also lead to personal criminal prosecution

iv. I understand and adhere to the requirements of the ICT policy on Security.

v. I understand and adhere to the requirements of the ICT Internet Access and Use policy

vi. I follow the directions of ICT Help Desk relating to their use of ICT facilities

vii. I undertake to ensure that my PASSWORD is kept confidential, and acknowledge that unauthorised use of my personal USER ID may result in the integrity of the system being compromised. I further accept that I am responsible for ensuring my personal USER ID is not shared and is only used for proper and authorised activities, and I am accountable for any actions undertaken using my USER ID

CONTACT INFORMATION

Date: ……Time……..
Dept/Section/Unit:…….

Name of Officer:…….
Position……

Authorised By
(**Supervisor**):Name……Position……
…

Signature……Date……..…

Original: **ICT Department**
2nd Copy: **Requesting Officer**

Appendix C Authorisation to access documents

MINISTRY OF HEALTH

INFORMATION & COMMUNICATION TECHNOLOGY UNIT

AUTHORISATION TO ACCESS DOCUMENTS FORM

The following must be completed by the person making the request and signed by their supervisor before access can be permitted.

CONTACT INFORMATION

Date: ……..
Dept/Section/Unit:…….

Name of Requesting
Officer:…….Position……

Authorised By (**Supervisor**):Name……Position……

Signature……Date……..…

Please supply the following details:

User id of computer profile to be accessed	
Is user still a member of MoH (yes/no)?	
Documents to be accessed, including its location.	
Reasons for this request. This **must** include an explanation of why a delay in access would be detrimental to MoH's interests.	
Intended duration of the proposed activities.	
The names and job titles of those who will access the stored material	

Original: **ICT Department**
2nd Copy: **Requesting Officer**
3rd Copy: **Computer Owner**

****The owner of the stored material must be given a copy of this form, a list of material accessed and a copy of the logged actions.**

Appendix D Software Installation request form

MINISTRY OF HEALTH

INFORMATION & COMMUNICATION TECHNOLOGY UNIT

SOFTWARE INSTALLATION REQUEST FORM

CONTACT INFORMATION

Date: ……..
Dept/Section/Unit:…….

Name of Requesting
Officer:…….Position……

Authorised By (**ICT**):……..
Date……..…

SOFTWARE INFORMATION (USER)

TYPE REQUESTED: ***Tick what is applicable***

- **New Software Installation.** **.**
- **Reinstallation of previous /corrupt software.**
- **Installation of new version of existing software.**

WHAT TYPE OF SOFTWARE SHOULD BE INSTALLED (USER)

Name of
Software:……..

Version:……

Platform on which to be installed:…….....Location:.....

Description of
Use:……..

Approved By: Name/Position:…….
Signature:……

Date:……..

Original: **ICT Department**
2nd Copy: **Requesting Officer**

Appendix E Equipment Support form

MINISTRY OF HEALTH

INFORMATION & COMMUNICATION TECHNOLOGY UNIT

EQUIPMENT SUPPORT LOG FORM

The following must be completed by the person making the request and signed by their supervisor before ICT can work on the equipment.

CONTACT INFORMATION

Date: ……Time……..
Dept/Section/Unit:…….

Name of Requesting
Officer:…….Position……

Authorised By
(**Supervisor**):Name……Position……
…

Signature……Date……..…

Please supply the following details:

brief description of the problem	
Serial Number of MOH Equipment	
Model and type of the Equipment	

Original: **ICT Department**
2nd Copy: **Requesting Officer**
3rd Copy: **Computer Owner**