LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
HEALTH

Information and Communication Technology Policy Handbook

Document Information

File Name	Information and Communication Technology Policy Handbook
Document Owner	GITO
Issue Date	Date of Approval

Document History

Version	Date
1.1	20-Nov-12
1.2	30-Sept-13
1.3	14-Jan-21
1.4	22-Feb-22
1.5	25-Jan-23

Approval

22/02/2023

Acting Head of Department **Date**

Table of Contents

1. Executive Summary....8
2. Introduction....9
3. Regulatory Framework....9
4. Definitions....10
5. ICT Policies Objectives....16
   - 5.1 ICT security policy....16
   - 5.2 Change control policy....16
   - 5.3 Acceptable usage of computer policy....16
   - 5.4 E-mail usage policy....16
   - 5.5 Internet usage policy....17
   - 5.6 User-ID and password policy....17
   - 5.7 ICT Patch Management Policy....17
   - 5.8 Data Back-Up and Restoration Policy....17
   - 5.9 Wireless Access Policy....17
   - 5.10 ICT Firewall Policy....17
   - 5.11 Virtual Meeting Policy....17

   The Virtual meeting policy shall provide guidance when officials hold and participate in virtual meetings....17
6. ICT Security Policy....18
   - 6.1 Introduction....18
   - 6.2 Policy Statement....18
   - 6.3 Policy Objective....18
   - 6.4 Scope of Application and Enforceability....18
   - 6.5 Key Policy Principles....18
   - 6.6 Compliance Monitoring....19
   - 6.7 Access Control and Authorization....19
   - 6.8 Care of ICT Equipment....19
   - 6.9 Information Security Components....20
7. Change control policy....23
   - 7.1 Introduction....23
   - 7.2 Scope....23
   - 7.3 Purpose of Policy....23
   - 7.4 Policy Statements....23

7.5 Procedures 24
8. Acceptable use of computer policy 25
8.1 Rationale 25
8.2 Scope 25
8.3 Responsibilities 25
8.4 Policy Statements 25
9. E-mail Usage Policy 28
9.1 Rationale 28
9.2 Scope 28
9.3 Responsibilities 28
9.4 Policy Statements 29
10. Internet usage policy 33
10.1 Purpose 33
10.2 Scope 33
10.3 Responsibilities 33
10.4 Policy Statements 33
11. User ID and Password Policy 36
11.1 Rationale 36
11.2 Background 36
11.3 User account management procedures 36
11.4 User registration 36
11.5 Modification/changes 37
11.6 User deregistration 37
11.7 Review of user access rights 37
11.8 Privilege management 38
11.9 User responsibilities 38
12. ICT Patch Management Policy 41
12.1 Rationale 41
12.2 Purpose 41
12.3 Scope 41
12.4 Risks 41
12.5 Policy Statement 41
13. ICT Data Back-Up and Restoration Policy 43
13.1 Purpose 43

13.2 Scope 43
13.3 Policy Statement 43
13.4 Enforcement 43
13.5 Back-Up Tools 43
13.6 Schedule 44
13.7 Retention 44
13.8 The Backup Process 44
13.9 Offsite storage 44
13.10 Responsibilities 44
14. ICT Wireless Access Policy 45
14.1 Rationale 45
14.2 Purpose 45
14.3 Scope 45
14.4 Responsibilities 45
14.5 Policy Statements 45
15. ICT Firewall Management Policy 48
15.1 Introduction 48
15.2 Purpose 48
15.3 Scope 48
15.4 Policy statement 48
15.5 Requirements 48
15.6 Operations 48
15.7 Configuration 49
15.8 Audit and Compliance 50
15.9 Responsibilities 50
15.10 Change control 50
15.11 Monitor stability 50
15.12 Enforcement 50
16. Virtual Meeting Policy 51
16.1 Purpose 51
16.2 Definition 51
16.3 Legal Framework 51
16.4 Related Documents/Policies 51
16.5 Scope 51

16.6 Roles and Responsibilities 51
16.7 Virtual Meeting Procedure 52
16.8 Data Efficiency 54
17. Inception date 54
18. Review 54
19. Enquiries 54
Annexure A: Virtual Meeting Etiquette 55

Acronyms

Acronyms	Description
E-mail	Electronic mail
CAB	Change Advisory Board
COBIT	Control objective for Information and Related Technologies
GITO	Government Information Technology Officer
HDD	Hard Disk Drive
HoD	Head of Department
ICT	Information and Communication Technology
MEC	Member of Executive Council
OEM	Original Equipment Manufacturer
RAM	Random Access Memory
SITA	State Information and Technology Agency
User-ID	User-Identification
LAN	Local Area Network
WAN	Wide Area Network
ISP	Internet Services Providers
RFC	Request for Change
SSDI	Service Set Identifier
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
ID	Meeting Identity
MISS	Minimum Information Communication Standards

1. Executive Summary

For good governance and audit compliance, Limpopo Department of Health (LDoH) is required to develop and implement the ICT policies in all healthcare institutions / facilities across the province. These policies are meant to guide and govern ICT users in their responsibilities and what is expected of them in relation to the use of departmental ICT services and/or resources. The development and implementation of ICT policies is in line with the implementation of Control objective for Information and Related Technologies (COBIT) as a governance framework.

Numerous policies have been identified as critical to assist the ICT environment in preparation for its operations. These policies shall be in the form of a handbook and the handbook shall include the following;

- Security policy
- Change control policy
- Acceptable use of computer policy
- Email usage policy
- Internet usage policy
- User ID and Password policy
- Patch Management policy
- Data backup and restoration policy
- Wireless access policy
- Firewall Management Policy
- Virtual Meeting Policy

2. Introduction

The LDoH ICT Policy Handbook provides the policies for selection and use of ICT within the business which must be followed by all staff. It also provides guidelines LDoH will use to administer these policies, with the correct procedure to follow.

LDoH will keep all ICT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies.

Any suggestions, recommendations or feedback on the policies specified in this manual are welcome.

These policies apply to all employees

3. Regulatory Framework

This policy shall be read in conjunction with the following:

- Electronic Communications Act
- Constitution of Republic of South Africa
- King Ill Code on Corporate Governance
- Minimum Information Security Standards (MISS)
- National Archives and Records Service Act of South Africa
- Promotion of Access to information Act
- Public Administration and Management Act
- Public Finance Management Act
- Public Service Act
- Regulation of Interception of Communications and Provision of Communication-related Information Act
- SITA Act
- SITA Regulations
- Corporate Governance of ICT Policy Framework
- Information Technology Security Policy for Limpopo Provincial Administration

4. Definitions

7Zip	an application that is used for compressing and uncompressing files and user data.
A breach of Security	where a stated departmental policy or legal requirement regarding information security has been contravened.
Access Point	A hardware device that serves as a communications "hub" for wireless clients and provides a connection to the wired LAN.
Archiving	A collection of computer files that have been packaged together for backup, to transport to some other location, for saving away from the computer so that more hard disk storage can be made available, or for some other purpose
Audio Sessions	Internet technology can also allow users to receive audio feeds such as radio stations over the internet
Authentication	Verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by ICTs claimed source. Authentication techniques usually form the basis for all forms of access control to systems and or data;
Authorization	A function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular.
AVI / MPEG	The audio visuals such movies, videos etc.
Back-Up	The activity of copying files or databases so that they shall be preserved in case of equipment failure or other catastrophe
Category of change	Determines the difficulty and impact of the change requested, resources required to effect the change, the timelines as well as the level of authorization required

Chain letters	Consists of a message that attempts to induce the recipient to make a number of copies of the letter and then pass them on to as many recipients as possible.
Change Control process	The procedure that governs the implementation of any changes to an ICT system.
Client hardware or Software	An electronic equipment and software that is installed in a desktop, laptop, portable, or other computing device to provide a LAN interface to a wireless network.
Computer User(s)	Persons who have access to or use of the LDoH Equipment, Communication Facilities or Communications.
Confidentiality Breaches	Unauthorized disclosure of confidential, proprietary or trade secret information such as when the employee secretly trade a product design specification, sales data and information of which departments are competing for, the sender and recipient may be charge for trade secret theft.
Cookies	Web sites use 'cookies' to simulate a continuous connection to that site. This makes ICT more convenient for users by allowing them to visit pages within a site without having to reintroduce them with each mouse click.
Coverage	Means the geographical area where a baseline level of wireless connection service quality is attainable.
Critical Update	A broadly released fix for a specific problem, addressing a critical, and non-security related bug
Damage Reputations	Distortion, interruption or unwanted disclosure of messages such as badly written e-mail or e-mail containing unprofessional remarks shall cause the recipient to have a bad impression of the department the sender is representing.
Distribution List	Creation on the messaging infrastructure to group users together in a group that shall receive common e-mail information. Distribution groups are created to assist users in sending e-mail messages to a large number of users.
Driver	Software required by the operating system to make a piece of hardware function.

E-mail Infrastructure	A computing facilities, services and network systems such as computers, computer data processing or storage functions service, servers, input/output and connecting devices related to computer records, programs, software and documentation to send e-mail message.
E-mail Attachment	A file attached to the e-mail message.
E-mail Auditing	When LDoH e-mail users are scanned after the actual transmission.
E-mail interception	This is where the e-mail is intercepted and scanned during the transmission.
E-mail SPAM	The word SPAM relates to information that is of no importance to email recipients. SPAM is an e-mail intruder that shall use the LDoH email infrastructure to send non relevant business information to large number of users. SPAM is illegal and users shall be aware of SPAM information such as non-business related advertisements and non-business related E-mail messages.
Emergency change	A change that is urgent and required for the proper functioning of a system and cannot wait for a change control committee to take place before ICT can be implemented.
Encryption	Process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make ICT unreadable to anyone except the owner or recipient.
Firewall	Firewall technology is used to protect the LDoH internal ICT services from malicious activity on the internet.
Guidelines	A general statements designed to achieve the policy objectives by providing a framework within which to implement procedures, whereby standards are mandatory, guidelines are recommendations;
Hot-fix	A single package composed of one or more files used to address a problem in a product.

Illegal Software	Software with no LDoH legal software license. LDoH ICT is responsible for all software licenses. LDoH shall be audited annually to find all legal and illegal software. LDoH may be fined for all illegal software that is installed on LDoH user's workstations.
Illegal Software	Refer to the software that is not registered nor has no license to be used by the department.
Information Security Officer	An employee appointed and employed by LDoH to enforce and manage this Policy.
Information Resource	Refers to all computer and related resources that require authentication. These resources include computer data capture, reports, access to on-line display terminals, magnetic and other storage media, e-mail archives, web sites and other content management systems, personal computers either connected or standalone used by the department. Other devices included in the information resource description are; personal electronic organizers, distributed systems, servers, mainframes, fax facilities, telephone access, related telecommunication resources for example routers. Additionally, ICT is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information;
Information Services	A unit responsible for providing computer related services. These services shall include all aspects of management in the context of the Information Resource;
Interference	Degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.
Internet Chat rooms	These are created in the internet to provide a central point for users that communicate via text on different issues.
Internet Monitoring tools	A tool that provides information on the usage of internet and block unwanted sites from the internet user computer.

Internet Services Providers	Is used to provide Internet connectivity to users all over the world. ISP provides the interlinking services to create internet access.
JPG / PEG	Pictures downloaded from the digital camera or from Internet.
Legal liability	These are legal costs and penalties incurred or paid by LDoH when distribution of viruses or other harmful programs are sent through LDoH e-mail system as these harmful programs could threaten work environment for other employees.
Letter-bomb	Resending the same e-mail repeatedly to one or more recipients which interfere with the recipient's use of mail.
Loss of productivity	This is when inappropriate usage of e-mail system is of a great concern where employees waste their productive time through reading or sending E-mails, which does not contain business related information.
Macro's	Macro's are used in documents and spread sheet to perform predefined work statements and calculations. Viruses can also use Macro functionality to introduce malicious actions.
Mailbox	It is the holding place for E-mail that is received and transmitted.
Media Retention	Protect backups from being overwritten until the specified. number of days has elapsed.
Media streaming	Is a technology that is used to provide media services via the internet that provides video type services.
Password	A string of characters used to authenticate a person's identity in the context of a situation. This authentication mechanism is used to gain access to either private and privileged, or shared data.
Patch or fix	A release of software that includes bug fixes or performance enhancing changes.
Peer to Peer Network	Denoting computer networks in which each computer can act as a server for the others, allowing shared access to files and peripherals without the need for a central server.

Peripheral ICT Equipment	ICT equipment that connects to the computer from the outside casing
Privacy	The condition that provides for the confidentiality of patient data and staff communications transmitted over a wireless network.
Procedures	Explains specifics of how the policy and the supporting standards and guidelines shall actually be implemented in an operating environment;
Restoration	A process that involves copying backup files from secondary storage (backup media) to disk
Security Patch	A broadly released fix for a specific product, addressing security vulnerability
Service release or service pack	A release of software that bundles together several patches and/or updates to provide a clear benchmark or level of release (e.g. Service Pack I).
Service Set Identifier (SSDI)	May be used as a relatively insecure security key for a WLAN, somewhat like a password. If the SSID is set in the Access Point, then only client wireless cards configured with the same SSID may connect to that Access Point.
Spam	Computer Spam is the electronic equivalent of Junk mail
Standards	Mandatory activities, actions, rules, or regulations designed to provide policies with the support structure, and specific direction they require to be meaningful and effective. They are often expensive to administer and, therefore, shall be used judiciously;
Update	A release of software that adds new functionally to an earlier version.
User Account	Determines which user rights and access permissions you have on the computer and allows a user to authenticate to system services through the computer and be granted authorization.
User-ID	A unique identification of LDoH workstation users. The User-ID is used to gain access to Information Technology systems. User-IDs are also used to audit workstation user's activities.

Version or build	Software that has a numeric or named attribute denoting ICTs maturity or age
Virus / Trojan Horse / Worm or email bomb	This is a form of potentially disruptive, dangerous malicious program.
Viruses	Viruses are malicious programs created to disrupt computer services.
Websites	Internet servers that provide browse pages with information, data and services to users on the internet.
Wired Equivalent Privacy (WEP)	Provides limited security to a wireless connection by encrypting all data transmitted between the computer and the access point.
Wireless Infrastructure	Wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.
Wireless Local Area Network (WLAN)	Provides the functionality of a wired LAN without the physical constraints of the wire.

5. ICT Policies Objectives

5.1 ICT security policy

The objective of this policy is to ensure confidentiality, integrity and accessibility of information and systems in the Limpopo Department of Health.

5.2 Change control policy

The policy shall ensure that all changes are performed in a manner that introduces minimal disruption to the department's applications, systems and network.

5.3 Acceptable usage of computer policy

The Information and Communication Technology equipment is provided by the Department specifically to enable LDoH employees to effectively and efficiently perform their daily duties. This policy shall clearly define the business requirements to utilize computer systems.

5.4 E-mail usage policy

The e-mail policy provides guidance about acceptable use, for the purpose of sending or receiving email messages and attachments, of any ICT facilities, including hardware, software and networks, provided by the department. The e-mail and messaging policy ensure the appropriate use of LDoH e-mail system

and make Departmental e-mail users aware of what LDoH deems as acceptable and unacceptable use of ICTs electronic messaging system.

5.5 Internet usage policy

The Internet Usage policy ensures the appropriate use of the department internet facilities and makes LDoH users aware of what is deemed as acceptable and unacceptable use of the internet infrastructure.

5.6 User-ID and password policy

The User-ID and Password Policy shall mitigate exposure the LDoH might encounter to legal risk and liability. This policy shall further protect the departmental resources on the network computers by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords. Information access needs to be managed via user based authentication mechanisms. Controlling access is necessary to ensure that appropriate information resources are protected.

5.7 ICT Patch Management Policy

The policy on vulnerability and patch Management assist in keeping the components that form part of information technology infrastructure (hardware, software and services) up to date with the latest patches and updates.

5.8 Data Back-Up and Restoration Policy

The Data Back-Up and Restoration policy shall define the standards and processes that shall be followed in the LDoH for the backup of data and or e-HIS system.

5.9 Wireless Access Policy

Wireless Access Policy shall guide the deployment standard and integrity of wireless networking on the LDoH to ensure reliable, compatible, and secure operation.

5.10 ICT Firewall Policy

Firewall Policy shall describe how the firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access.

5.11 Virtual Meeting Policy

The Virtual meeting policy shall provide guidance when officials hold and participate in virtual meetings.

6. ICT Security Policy

6.1 Introduction

The Limpopo Provincial LDoH recognizes the value and strategic nature of information and the systems and ICT infrastructure that facilitate the secure transmission of the information. LDoH is faced with security threats from a wide range of sources, including computer assisted fraud, espionage, sabotage, vandalism, viruses, computer hacking and denial of service attacks. Departments of Health in the country are facing high number of litigation cases. Some of these cases are lost due to missing physical medical records. To prevent this, departments are moving to electronic medical records which exposes the LDoH to more cyber security threats. The ICT security policy shall secure management of information and systems, minimize the risk of unauthorized access and loss of information.

6.2 Policy Statement

ICT shall provide the computerized systems to ensure confidentiality, integrity and availability of information for the LDoH.

6.3 Policy Objective

The objective of this policy is to:

- protect the department's information and any client information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability;
- encourage the employees of the department in maintaining an appropriate level of awareness, knowledge and skills to allow them to minimize the occurrence and severity of ICT security incidence
- Establish the minimum requirements for any applications and information systems developed or purchased by LDoH to support its business operations.

6.4 Scope of Application and Enforceability

The policy is applicable and enforceable on all employees of the department and contractors using, accessing, storing, transmitting or overseeing the departmental resources directly or by means of a personally acquired device.

- The Policy applies to all personal and non-personal data or information, information systems, Information and Communications technology (ICT) networks and applications.

6.5 Key Policy Principles

- It essential to maintain the security of LDoH business applications for the protection of its information assets against internal, external, deliberate or accidental threats that exploit software vulnerabilities
- Any application or system owned and operated by LDoH must be secured by implementing minimum requirements of this policy

- Any information system or software tool that LDoH intends to implement must be assessed for vulnerabilities and such vulnerabilities be remedied before implementation into the production deployment

6.6 Compliance Monitoring

To ensure that resources are not abused, the department reserves the right to monitor a selection of messages and material sent across the network or stored in computers connected to ICTs network and take appropriate action if it comes to the attention of the department that these resources were abused. The GITO unit shall perform the network monitoring function.

- Every user shall acknowledge that the department has a right to monitor a selection of messages sent across the network as well as information stored on the department's computers and take appropriate disciplinary action where contravention of this policy is observed.
- Authorized personnel in the GITO unit may examine computing resources, communication systems, files, emails and or printing listings for reasons including but not limited to:
    - Troubleshooting hardware and/ software problems
    - Preventing or investigating unauthorized access or system misuse
    - Ensuring compliance with software copyright and distribution policies
    - Complying with legal and regulatory requests for information

6.7 Access Control and Authorization

- Restricting access to information and application functions must be based on identity of users and/or membership in certain group after authentication.
- Applying the following guidelines must be considered in order to support access restriction requirement:
    - Providing menus to control access to application system functions.
    - Controlling the access rights of users, e.g. read, write, delete and execute.
    - Controlling access of other applications.
    - Ensuring that outputs from applications systems handling classified information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations, this must include periodic reviews of such outputs to ensure that redundant information is removed; and
    - If individual authorization is used, these must expire and require renewals on a periodic basis

6.8 Care of ICT Equipment

- ICT hardware shall be treated with care and only used in accordance with proper operating instructions. All faults shall be reported to the helpdesk.

- Users shall not by deliberate or careless act or omission jeopardize or seek to jeopardize the integrity of any ICT equipment or software or information stored in or accessed through ICT.
- Every user issued with departmental ICT equipment or granted access to departmental ICT resources shall sign the user acceptance form.

6.9 Information Security Components

Systems, processes and procedures to ensure the protection of departmental information and network against attacks and intrusions shall be put in place and managed by the GITO unit.

6.9.1 Disaster recovery plan

A disaster recovery and business continuity plan shall be put in place to ensure continuity of service in the event of a disaster

6.9.2 Asset Management

Every unit shall keep an up-to date record of all ICT equipment allocated to employees and contractors in the unit. Every unit shall keep an accurate record of all movement of ICT equipment and software from office to office or from one user to another in or outside the unit. Inventory of all ICT equipment and software shall be kept by ICT infrastructure.

6.9.3 Change Control

A change control committee shall be established to manage, approve and ensure implementation of all changes in the network.

6.9.4 Responsible Use of e-mail, Intranet and Internet

Access to Internet, Intranet and email shall be provided to employees and authorized users as a working tool and shall be used to achieve this primary purpose.

6.9.5 Copyright

Computer programs installed on the departmental computers are protected by copyright laws. Users shall not infringe upon these copyrights by copying such software or data or using the software without authorization from the copyright owner or license owner.

6.9.6 Software Licenses

All software installed on departmental computers is governed by license agreements between the department and the license owner. Users shall not infringe on these licenses by copying the software and using ICT without permission from the original license owner. All employees shall not install any unlicensed or pirated software on departmental computers.

6.9.7 Privacy

All employees, contractors and authorized users of the departmental systems shall ensure that information or records in their care are handled in terms of the Minimum Information Security Standards. Access to personal information shall be limited to authorized users for approved purposes.

6.9.8 Intellectual Property rights

All software and systems developed for the department (whether by a contractor, employee or service provider) and paid for by the department shall become the intellectual property of the department, unless otherwise stated in the contractual agreement.

6.9.9 Personal use of ICT resources

Employees and authorized users are permitted limited use of ICT resources for personal purposes to a level that is reasonable and not detrimental to the main purpose they were procured for or contributes towards enhancement of productivity.

6.9.10 Server and computer rooms

Access to server rooms shall be controlled and limited to authorized personnel only. Computer rooms shall have an access control system implemented to ensure that unauthorized personnel do not gain entry into the facilities. Computer rooms shall have adequate physical security to ensure that no unauthorized access/ entry is gained into them such as ensuring that the roofs are sealed and made of concrete.

6.9.11 Internet Usage

Internet shall be used primarily for the performance of the work of the department. Access to the internet shall be granted to authorize personnel only.

6.9.12 E-Mail Usage

E-Mail is a work tool and shall therefore be used for work related purposes. Any forwarding of messages with pornographic, racist and derogatory content is prohibited

6.9.13 User Account Management

All users have a responsibility to keep their passwords and login credentials secret. All transactions performed using their credentials shall be deemed to have been executed by them. All accounts that have been inactive for a period longer than days shall be deactivated. A new employee in the department shall be provided with access to ICT policy handbook. Human Resources management unit shall inform ICT about the staff turnover of the department.

6.9.14 Back up and Disaster Recovery Management/contingency planning

To ensure prevention of information and data loss in the event of a disaster/ failure, ICT shall maintain regular back-ups of departmental information and have ICT service continuity and disaster recovery plan which shall be tested at least once every year.

6.9.15 Password Management

A password shall include a combination of at least Seven (7) alphanumeric (numbers and alphabets as well as special characters e.g. &, * # among others) characters. A password shall be valid for at most 30 days. Users shall not be required to change password where Multi Factor Authentication has been enabled. Previous twelve passwords shall not be used.

6.9.16 Virus Protection

ICT shall ensure that there is an up-to-date anti-virus protection available and that all workstations are regularly updated with the latest anti-virus definitions. A regular scanning of all workstations shall be done to ensure removal of any suspected viruses in the workstations. Users shall not be allowed to disable scanning of the anti-virus software on their computers. All suspected virus attacks shall be reported immediately to ICT.

6.9.17 Access Control

Access control to computer systems shall be approved by the system owner. A register of all users including their access rights together with the forms for approval shall be kept. Access rights to systems shall be commensurate with the job functions and responsibilities of the users. User access rights shall be reviewed at-least twice a year to ensure they are still appropriate. All systems shall have system owners and administrators appointed in writing. All users that have left the service of the department shall have their credentials removed from the system upon receipt of notification of such departure.

6.9.18 Software security

The use of unauthorized and unlicensed software is prohibited. ICT shall remove any unauthorized software without consulting the user.

6.9.19 Network security

Firewalls, intrusion detection and prevention solutions shall be implemented to protect the network against intrusions and cyber-attacks. All attempted intrusions shall be monitored and reported to the ICT Security office.

6.9.20 Incident Reporting and Management

All incidents of security breaches and attempted intrusions shall be reported to the ICT Security Office.

6.9.21 Vendor demonstrations and Proof of concepts

All demonstrations by vendors shall be done on the vendor's equipment and not on the department's equipment.

6.9.22 Auditing and Monitoring

A regular audit and monitoring of compliance to the policy shall be performed.

6.9.23 Removable media

All removable media (CDs, memory sticks etc.) shall be scanned for viruses by ICT before being used on departmental equipment. Autorun command shall be disabled.

7. Change control policy

7.1 Introduction

The LDoH has a significant investment in ICT assets. These assets are critical for the enablement of service delivery by the department. Like any organization which manages complexity, the departmental systems shall undergo changes of various forms and for a variety of reasons. This policy is aimed at providing guidance and direction in the management of changes in the ICT environment from software configuration changes through to new infrastructure deployment.

7.2 Scope

The Policy is applicable to all changes in the ICT environment, from installation of a single device to the departmental network to performing a system or network upgrade. The policy deals with requirements for communicating, implementing, documenting, managing and reporting changes performed on the ICT infrastructure, systems and applications.

7.3 Purpose of Policy

The policy is aimed at ensuring that all changes are performed in a controlled manner to reduce disruptions to the ICT services and that proper authorization is granted before changes are deployed to production. This policy also aims to ensure that adequate testing is performed before changes are implemented

7.4 Policy Statements

All changes made to the departmental systems, infrastructure and applications that may affect normal operations shall undergo a process of approval by the Change Advisory Board (CAB) before being deployed. All changes to any system, device or application shall be tested and approved before being deployed. The test results shall be documented and submitted to the CAB as part of the request for

change. Duties shall be segregated for implementation of changes to ensure that the requestor of the change doesn't authorize or approve that change request.

7.5 Procedures

7.5.1 Minor Changes

ICT handles many changes to information systems on a daily basis and most of them do not justify a formal approval process. In particular, changes to desktop or notebook computers that only impact on a single user may be performed without prior approval, provided that the other stipulations of this policy are adhered to. However, minor changes to Servers, Network Applications and the Network Infrastructure shall be recorded.

7.5.2 Major changes

- A request for upgrade or modifications shall be made in writing for any information system by completing a change request form.
- A recommendation for the change to be effected shall be made by the system owner or supervisor of the requestor of the change
- The CAB shall meet to review and approve the change request
- All changes, approvals and refusals shall be documented and stored in a central location for future use
- On approval of the change, communication shall be sent to all affected users informing them of the change, effected service(s), downtime and expected time for restoration of service
- On restoration of service(s), a communication shall be sent out to all affected users informing them of the completion of the change implementation
- A schedule of all planned changes shall be maintained for all changes that are foreseen

7.5.3 Emergency changes

- All emergency changes shall be approved by the GITO or a relevant delegate on the motivation of the requestor
- All emergency changes shall be recorded and have their documentation stored in a central location
- The emergency changes shall be communicated to all affected users informing them of the change
- On restoration of service(s), a communication shall be sent out to all affected users informing them of the completion of the change implementation

8. Acceptable use of computer policy

8.1 Rationale

The Acceptable Usage of Computer policy is devised to protect the LDoH Information System of business unit and ICTs employees in respect of the usage, maintenance and control of the Information Technology equipment by determining the principles and rules, which govern the use of computer systems.

The Information Technology equipment is provided by the Department specifically to enable LDoH employees to effectively and efficiently perform their daily duties. This policy is clearly defining the business requirements to utilize computer systems.

8.2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct LDoH business or interact with internal networks and business systems, whether owned or leased by LDoH the employee, or a third party. All employees, contractors, consultants, temporary, and other workers are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with LDoH policies and standards.

8.3 Responsibilities

All users shall be responsible for the prevention of their computers and/or laptops from theft. Regular awareness campaigns shall be conducted to ensure that staff in the department are conscious of the Acceptable Usage of Computer Policy and understand the consequences if breached.

8.4 Policy Statements

8.4.1 General Use and Ownership

- Users shall be aware that the data they create on corporate systems remains the property of the department.
- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of LDoH proprietary information.
- Users may access, use or share LDoH proprietary information only to the extent it is authorized and necessary to fulfill their assigned duties.
- Only legally licensed software shall be installed on LDoH computers and servers.
- Software shall not be copied or installed without the permission or involvement of the ICT department.
- For security and network maintenance purposes, authorized individuals within LDoH may monitor equipment, systems and network traffic at any time.
- LDoH reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

8.4.2 Physical and Computer Security Guidelines:

- ICT shall configure all departmental computers with anti-virus protection software, which shall not be removed or disabled.
- Each LDoH employee shall be responsible for protecting their computers against virus attack by following ICT guidelines on scanning all incoming communications and media (if prohibited), and not disabling the anti-virus application installed on their computers.
- All data disks and files entering or leaving the department shall be scanned for viruses.
- All employees shall log off from the network and leave their computers on for anti-virus updates before leaving the office at night.
- Disguising or falsifying sources of electronic mail and other electronic communications with the intent of misleading, defrauding or harassing others by a LDoH employee is prohibited.
- Computers with sensitive information installed on the local disk drive shall be secured in a locked room or office during non-business hours.
- Equipment which is to be removed from LDoH property shall be approved in advance with the assets unit under Supply Chain Management and an inventory of this equipment shall be maintained in the assets register.
- All equipment removal from the premises including computers by the LDoH employee shall be documented, including makes, manufacturers and serial numbers on assets supplied form, and a copy of this form shall be filed in the assets registry folder.
- Passwords shall be kept secured, sharing of user-ID (Persal numbers) and password is prohibited.
- All portable computers and desktop computers shall be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by pressing (control > alt >delete) when the computer shall be unattended.
- If an employee leaves the department, he or she shall return the equipment (laptop and/or Desktop) to LDoH on or before the last day of employment.
- Employees may be exempted from these restrictions during the course of their legitimate job responsibility (e.g. systems administration staff may have a need to disable the network access of a computer if that computer is disrupting production services).
- All datacenter with at least 4 servers should meet the requirements for tier 1 data center.

8.4.3 The following activities are strictly prohibited, with no exceptions:

- Using excessive network bandwidth and excessive printing.
- Modifying system facilities, operating systems, or disk partitions without proper authorization
- Attempting to access private information without proper authorization.
- Attempting to crash up LDoH computers or networks.
- Damaging or vandalizing LDoH computing facilities, equipment, software or computer files.
- Eating, drinking, and smoking in proximity to information processing facilities

8.4.4 E-mail Communications Security

- Postage done by LDoH employees through e-mail address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the department, unless posting is in the course of business duties.
- All computers connected to LDoH network, whether owned by an employee or the department, shall continually run approved anti-virus software.
- Employees shall use extreme caution when opening e-mail attachments received from unknown senders as these may contain viruses.

8.4.5 The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited e-mail messages, including the sending of 'junk mail' or other advertising material to individuals who did not specifically request such material (email Spam).
- Creating or forwarding 'chain letters' or other 'pyramid' schemes of any type.

  Posting the same or similar non-business-related messages to large numbers of employees;
- Sending unsolicited bulk electronic mail or distributing unsolicited material though group communication channels

8.4.6 Application, System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or department protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited

  to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by LDoH.
- Unauthorized copying of copyrighted material including, but not limited to copyrighted sources, copyrighted music, and the installation of any copyrighted software for which LDoH does not have an active license, is strictly prohibited.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).
- Under no circumstances, an employee of LDoH is authorized to engage in any activity that is illegal under local, government, or international law while utilizing LDoH or owned resources especially when connected to the department network.
- Security breaches or disruptions of network communication which include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Circumventing user authentication or security of any computer, network or account.
- Computer equipment, software, or peripherals owned by the LDoH shall not be modified or removed without proper authorization.

- Using any program, script or command for sending messages of any kind, with the intent to interfere with, or disable a user's terminal session, through any means, locally or through the internet and intranet.
- Providing confidential information about LDoH to third parties without permission.

8.4.7 Lost, damaged or stolen laptops

LDoH employees shall be liable and responsible for the cost and expenses to replace lost, damaged or stolen laptops should the he/she be found to have been negligent and such liability shall be calculated as follows:

- First claim — 20% of value of claim;
- Second claim — 50% of value of claim; and
- Third claim — 100% of value of claim.

9. E-mail Usage Policy

9.1 Rationale

The e-mail policy provides guidance about acceptable use, for the purpose of sending or receiving email messages and attachments, of any ICT facilities, including hardware, software and networks, provided by the department. The policy also describes the standards that users are expected to observe when using these facilities for e-mail and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities.

The purpose of the LDoH e-mail and messaging policy is to ensure the appropriate use of LDoH e-mail system and to make Department e-mail users aware of what LDoH deems as acceptable and unacceptable use of ICTs electronic messaging system.

9.2 Scope

The e-mail policy applies to all LDoH computer users, staff requiring access to electronic equipment and consultants requiring access to information for the purpose of sending, receiving, distributing, storing and retrieving of e-mails messages and attachments, delivering outputs through e-mail from any ICT facilities in any access mechanism.

9.3 Responsibilities

The ICT department shall be responsible for the overall e-mail and messaging policy. Regular awareness campaigns shall be conducted to ensure that all staff in the department are aware of the e-mail policy and understand the consequences if breached. The LDoH messaging infrastructure shall be managed and controlled by the network administrator. Therefore, the department computer users shall be responsible for e-mail policy and other related policy compliance.

9.4 Policy Statements

9.4.1 E-mail Massaging Guidelines

- Private use of the LDoH e-mail and messaging infrastructure is permitted but this is subject to ICT control. Abuse of this privilege may be regarded as misconduct.
- The LDoH messaging system is abused when the following rules are not adhered to:
  - When users forward any non-departmental business-related e-mails
  - When users create or forward any personal e-mail jokes, music files, video files and junk e-mail which also contribute on network overload.
- All e-mails created, sent, stored, forwarded, or printed are the property of LDoH.
- Through using e-mail, department users shall be deemed to have read, understood and agreed to the policies relating to LDoH e-mail systems.
- Users shall only forward classified or confidential messages to other staff members that are permitted or authorized to receive such information.
- Department e-mail users shall stay alerted to the messaging warnings regarding virus from e-mail systems and report to LDoH service desk.
- Delete any e-mail enclosed viruses, BEFORE opening, particularly if documents containing executable programs being sent. If an employee opens a message and are prompted to "Enable or Disable macros" an employee shall select "Disable" and scan for viruses. If any viruses are found, then an employee shall notify the system administrator and LDoH service desk at Helpdesk@dhsd.limpopo.gov.za. If none are found, you may utilize the attachment.
- If an employee gets an attachment via e-mail which is unsolicited or of unknown origin, scan the file using the approved anti-virus software. It is advisable to delete any unknown e-mail and not reply to the sender. For any assistance regarding attachment scanning please contact LDoH service desk.
- Avoid unnecessarily large distribution lists. Department e-mail users shall rather create smaller distribution lists.
- Distribution groups can be created in the department using the proper request for change procedure;
- Log a call with the LDoH service desk to create the required distribution lists;
- Grouping of Distribution lists can be requested by units and user groups
- Ensure that the content of the message is not ambiguous and that there is nothing unlawful about the transmission or content of your message.
- Each directorate shall add the confidential, trade secrets and proprietary information to the documents.
- LDoH user who shall not read or respond to received e-mail massages within a period longer of 2 days shall enable the Out of Office reply function. Contact the LDoH service desk for assistance regarding the Out of Office setup.

- It is recommended that unwanted e-mails are regularly deleted and important e-mails are moved to appropriate folders. All personal e-mails shall be moved to appropriate folders created on the local machine, to free up space, and official departmental emails shall be kept in the inbox, thus the important mail shall always be available for online viewing.
- E-mail account not used for 90 days shall be disabled.
- Employees shall regularly move important information from electronic mail message files to word processing documents, databases, and other files, as e-mail messages and attachments may be erased periodically, either accidentally or as part of normal archiving and file maintenance functions.
- If employees receive unwanted and unsolicited e-mail (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they shall contact the system administrator and the service Helpdesk.
- Avoid sending messages with attachments larger than 3MB for external internet e-mail. Large attachments can be compressed and uncompressed using compression utilities such as 7Zip.

9.4.2 E-mail Communications Security

- Postage done by LDoH employees through e-mail address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of, unless posting is in line business duties.
- All computers used by the employee that are connected to the LDoH internet, intranet and extranet, whether owned by the employee or the department, shall be continually executing approved virus-scanning software.
- Employees shall use extreme caution when opening e-mail attachments received from unknown senders as these may contain viruses.

The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited e-mail messages, including the sending of 'junk mail' or other advertising material to individuals who did not specifically request such material (email Spam).
- Creating or forwarding 'chain letters' or other 'pyramid' schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of employees; this is called a Newsgroup Spam.
- Sending unsolicited bulk electronic mail or distributing unsolicited material though group communication channels

9.4.3 Unacceptable Usage of E-mail

ICT users are prohibited to display or transmit:

- Offensive, defamatory, discriminatory or harassing material;
- Sexually explicit or other offensive images or jokes;
- Unlicensed copyright material;

- Non- business-related video and image files;
- Any message which would be deemed unlawful pursuant to the applicable law of any governing jurisdiction;
- Confidential, proprietary or trade secret information outside without authorization;
- Private and personal advertisements;
- Chain letters;
- E-mail notices concerning virus or harmful code warnings to other LDoH employees.
- The LDoH e-mail and messaging infrastructure shall not be used for politically motivated e-mails.
- When using electronic mail to communicate with people on the internet:
    - An employee shall not automatically forward internal mail to an internet site;
- When sending or forwarding e-mail to the internet, an employee shall not include the system User-ID's of any LDoH employees;
- An employee shall not use auto-reply functions to respond to an internet mail.
- Employees shall not use an electronic mail account assigned to another individual to either send or receive messages. Individuals that require other users to use their messaging infrastructure shall complete a request for change with the LDoH service desk.
- Users shall not, as a matter of course, forward confidential, trade secret or proprietary information to third parties without ICT being classified or encrypted. Confidential information is deemed confidential or departmental proprietary information when the following headings or subtext are present:
    - Confidential Information
    - Proprietary Information
    - LDoH Internal Information

9.4.4 Risks of E-mail

Since e-mail includes both the transmission and handling of sometimes sensitive information, care shall be taken to protect the message from unauthorized access. Threats can include the ability of individuals to change and copy information, or to distribute information to unauthorized parties. Users can also act anonymously, or with a fake identity, and spread information under an assumed name.

The use of LDoH messaging system shall be open to a number of commercial risks, including:

- Change or distribution of messages through error or negligence;
- Unauthorized use, processing or distribution of messages;
- Distortion, interruption or unwanted disclosure of messages;
- Infection with, and distribution of, viruses or other harmful programs;

- Unauthorized disclosure of confidential, proprietary or trade secret information; ⎯ Copyright infringement.

9.4.5 Messaging Disclaimer

The messaging disclaimer serves to protect the LDoH from e-mail breach of policy and the unauthorized transmission of LDoH confidential information. The e-mail messaging disclaimer shall be applied to all outgoing e-mails. The LDoH E-mail Messaging Disclaimer shall be as follows:

This message may contain confidential information and is intended only for the specified recipient. If you are not the specified addressee you shall not disseminate, distribute or copy this e-mail. If you have received this e-mail by mistake, please notify the sender immediately by e-mail and also delete this e-mail. E-mail transmission cannot be guaranteed to be secured or error-free as information could be intercepted, corrupted, lost, destroyed, late, incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the content of this message, which arise as a result of e-mail transmission. The LDoH shall not take responsibility for the e-mail user's personal views.

9.4.6 Size limits of Mailboxes, and E-mail attachments

The following limits apply to LDoH users:

Mailbox Size

The mailbox size for all users is at least 350MB. ICT will keep on determining the mailbox size informed by the available storage space. The following are the current size limits on email attachment;

- 5MB for outgoing and incoming emails
- 10MB for internal emails

9.4.7 E-mail Naming Convention

The following e-mail naming convention shall be applied and adhered to by all LDoH e-mail systems.

Username	The username is made up of the employee's Persal number
First Name:	Use only lowercase characters. Use the full first name, i.e., no nicknames, and do not use any middle names.
Last Name:	Use only lowercase characters. Use the full last name
Global Catalogue Display Name	First name, Last Name (Department)
E-mail Naming Convention	E-mail accounts policy naming convention shall be as follows: first name.surname@dhsd.limpopo.gov.za

10. Internet usage policy

10.1 Purpose

The purpose of the Internet Usage policy is to ensure the appropriate use of the department internet facilities and to make LDoH users aware of what is deemed as acceptable and unacceptable use of the internet infrastructure.

10.2 Scope

The internet usage policy applies to all LDoH employees who had been granted access to the internet. The Internet shall be used by LDoH employee and contractors to connect to customers, suppliers and other organizations. It is important to remember the following points:

- The Internet is used by millions of people worldwide.
- Unprotected information sent across the Internet may well be read by any number of unknown people.

10.3 Responsibilities

The LDoH infrastructure and policies shall be managed and controlled by the ICT unit in conjunction with State Information Technology Agency (SITA). LDoH users are responsible to adhere to internet usage rules. The Server administrator shall use the internet monitoring tool to regularly monitor the abuse and the ineffectiveness of the internet.

10.4 Policy Statements

10.4.1 Appropriate Use

Although the internet is an informal communication environment, the laws for copyrights, patents, trademarks etc. apply. LDoH users using the internet shall:

- Repost material only after obtaining permission from the source;
- Reveal internal confidential, proprietary and trade secret LDoH information on the internet only if the information has been officially approved for public release by the HoD.

The LDoH internet connection may be used for educational and research purposes.

10.4.2 Inappropriate Use

- The LDoH internet access shall not be used for any illegal or unlawful purposes.
- Internet access shall not be used for or by performing work for profit with LDoH resources in a manner not authorized by ICT
- The LDoH internet connection shall not be used for commercial or political purposes.
- Users shall not attempt to circumvent or subvert security measures on the LDoH's network resources, or any other system connected to or accessible through the Internet.

- LDoH users shall not use internet access for interception of network traffic for any purpose unless authorized by ICT.
- LDoH users shall not make or use illegal copies of copyrighted materials to read such copies on LDoH equipment or transmit these copies over the LDoH network.
- Illegal internet web sites include the following content:
- Offensive, defamatory, discriminatory or harassing material;
- Threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials;
- Sexually explicit or other offensive images or jokes;
- Download unlicensed copyright material;
- Non- business-related video and image files.

10.4.3 Risks of Internet

On the web, one of the real dangers is a possible loss of an employee's privacy or leakage of information about either an employee or the confidential LDoH documents and activities.

The following issues relate to an employee's privacy when surfing the web:

- When an employee visits a web site, the web site can identify where the internet connection originates. For example, if an employee uses the web from work, his/her activities can be identified as coming from the LDoH connection.
- Web sites can log all the activities, including any personal data as provided. The web site owner can associate an employee with this data on future visits. Some web sites do not respect data privacy laws and may make the information collected from an employee available to other organizations.
- Information known as "cookies" may be placed as a file on an employee's system by web sites. In some instances, other web sites can browse an employee's cookie file and find personal information. Cookies may be helpful but be aware that they persist until an employee manually erase them. an employee shall erase unwanted cookies regularly. Cookie settings may be changed in the browser preferences. An employee can send an email to Helpdesk@dhsd.limpopo.gov.za for further information about controlling cookies.
- Viruses are designed at best to cause some discomfort and at worst to cause the alteration and loss of data on a computer. Viruses pose a tremendous threat and can be introduced in a number of ways, particularly from files and programs downloaded from internet sources. ICT is therefore imperative that all computers accessing the internet use approved anti-virus software, and that this software is regularly updated.

10.4.4 Business Rules

- Whenever an LDoH user posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message shall be accompanied by words clearly indicating that the comments do or do not necessarily represent the position or views of LDoH.

- LDoH users can participate in business related internet chat rooms and business-related media streaming and audio sessions. LDoH software, documentation, and all other types of internal information shall not be sold or otherwise transferred to any party for any purposes other than the business purposes expressly authorized by LDoH.
- Authorization shall be obtained to transfer or post information on internet sites.
- LDoH users shall be prohibited from visiting illegal internet web sites. The ability for LDoH users to connect to a specific web site does not in itself imply that employees are permitted to visit the illegal Internet sites.
- LDoH users shall not up-load software which has been licensed by a third party, or software which has been developed by the LDoH, to any computer via the Internet unless authorization from ICT has been obtained.
- LDoH users are prohibited from connecting their personal computers to the departmental internet without authorization.

11. User ID and Password Policy

11.1 Rationale

The use of the User-ID and password Policy is to mitigate exposure the LDoH might encounter to legal risk and liability. This policy is designed to protect the departmental resources on the network by requiring strong passwords along with protection of these passwords and establishing a minimum time between changes to passwords. Information access needs to be managed via user-based authentication mechanisms. Controlling access is necessary to ensure that appropriate information resources are protected.

11.2 Background

LDoH shall protect its information assets from the risks created by both intentional and unintentional misuse of resources. The implementations of technology are diverse and complex (e.g. platforms, applications, operating systems, databases, email, internet, etc.) and all of them must be protected from unauthorized use. The risks can, however, be minimized by following the good user account management practices prescribed by the International Organization for Standardization, the International Electro Technical Commission on Information Technology — security techniques — Code of Practice for Information Security Management (ISO/IEC 27002:2005) and the Information Systems Audit and Control Association's guideline on access controls (G38). Criteria from these documents as outlined in this brochure could be of great value to the department when performing qualitative perspective, e.g. reputation impact, customer/public perceptions, regulatory effect and financial effect. Preventative controls shall therefore be implemented to minimize these risks to a level that is acceptable to the department. Detective controls are also required to secure the process. Proper user account management is one of the processes that can assist in achieving better information security, responsibility and accountability.

11.3 User account management procedures

These procedures shall cover all stages in the life cycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to information systems and services. All procedures shall be documented and formally approved (signed and communicated). Care shall be taken to ensure that access control responsibilities, e.g. access request, access authorization and access administration and monitoring, are segregated throughout the process.

11.4 User registration

A formal user registration procedure for granting access to information systems and services shall be in place. This procedure shall ensure the following, inter alia:

- A formally documented access request shall be completed and approved by the user's supervisor.
- The access request form shall make provision for adequate details regarding the user, supervisor, and type of access, approvals, etc. to be provided.
- Approval from the business/system owner shall be obtained before access is granted to business.

- The level of access granted to information and systems shall be appropriate in terms of the business purpose and shall be consistent with a departmental security policy, e.g. it shall not compromise segregation of duties (duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the department's assets).
- A written statement shall be issued to users explaining their access rights.
- Users shall sign statements indicating that they understand the conditions under which access is granted.
- Unique user identifications (IDs) shall be created that identify users and link their actions to their IDs.
- Redundant user IDs shall not be issued to other users.

11.5 Modification/changes

Changes in user status include changes of job function, roles, responsibilities and transfers within the department. A procedure shall be established to manage these changes in user status and shall include, inter alia, the following:

- Changes shall be communicated to information owners, users, super users, supervisors or any person/department responsible for defining, granting, changing or revoking access privileges.
- The access rights of users who have changed job function, roles, responsibilities, etc. shall immediately be removed or blocked.
- Procedures as for the registration of users shall be followed when the status of a user changes.

11.6 User deregistration

Access rights of users who have left the department shall be removed or disabled immediately.

11.7 Review of user access rights

The review of users' access rights is necessary to maintain effective control over access to data and information services. Users' access rights shall be reviewed as follows:

- At regular intervals After any changes such as:
    - Promotion
    - Demotion
    - Termination of employment
- When an employee moves from one section/division to another within the same department
- Authorizations for special privileged access rights shall be reviewed at more frequent intervals.
- Privilege allocations shall also be reviewed at more frequent intervals to ensure that no unauthorized privileges have been obtained.
- All changes to privileged accounts shall be logged for periodic review.

11.8 Privilege management

The allocation and use of privileges shall be restricted and controlled. Inadequate control of system administration privileges may be a major contributing factor in failures or breaches of systems. A formal authorization process shall be used to control the allocation of privileges in multi-user systems that require protection against unauthorized access. The following steps shall be considered:

- The access privileges associated with each system product, e.g. operating system, database management system and each application, as well as the users to which they need to be allocated, shall be identified.
- Privileges shall be allocated to users on a need to- use basis and on an event-by-event basis, i.e. the minimum required for their functional role and only when needed.
- An authorization process and a record of all privileges allocated shall be maintained. Privileges shall not be granted until the authorization process is complete.
- Privileges shall be assigned to a different user ID than that used for normal business activities.
- Changes to privileged accounts shall be logged for periodic review.

11.9 User responsibilities

Cooperation of authorized users is essential for effective security. Users shall be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

11.9.1 Password usage

Passwords are a basic control in verifying a user's identity before access is granted to an information system or a service according to the user's authorizations. Each employee shall be responsible for all the actions performed with his/her password, even if it is demonstrated that an action was carried out by another individual using the user's password. Users shall therefore follow good security practices in the selection and use of passwords and the following shall be kept in mind:

- Keep passwords confidential.
- Avoid keeping a record of passwords, e.g. hard copy or electronic file.
- Change passwords whenever there is any indication of possible system or password compromise.

Compose passwords that are:

- Easy to remember
- Of enough minimum length, e.g. six characters
- Not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone numbers, dates of birth, etc.
- Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries)
- Free of consecutive, identical, all-numeric or all-alphabetic characters.

- Change passwords at regular intervals or based on the number of times access has been obtained. The passwords for privileged accounts shall be changed more frequently than normal passwords.
- Avoid the reuse or cycling of old passwords. Change temporary passwords at first logon.
- Never share individual user passwords among users.

11.9.2 Unattended user equipment

All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities regarding the implementation of such protection. Users shall be advised to, inter alia:

- Terminate active sessions when finished, unless such sessions can be secured by an appropriate locking mechanism, e.g. a password-protected screen saver
- Log computers off at the end of a session (i.e. It is not enough to merely switch off the PC screen or terminal)
- Secure computers from unauthorized use by means of a key lock or an equivalent control, e.g. password access, when not in use.

11.9.3 User password management

The allocation of passwords shall be controlled through a formal management process and this process shall include the following requirements as a minimum:

- Users shall be required to sign an undertaking to keep personal passwords confidential. This signed statement may also be included in the terms and conditions of employment.
- If users are required to maintain their own passwords, they shall be provided with a secure initial password, which they shall be required to change immediately at first logon.
- Procedures shall be established to verify the identity of a user prior to providing the user with a new, replacement or temporary password.
- A secure procedure shall be followed when granting users temporary passwords and the use of unprotected (clear text) electronic mail messages shall be avoided.
- Temporary passwords shall be unique and shall conform to password standards.
- Users shall acknowledge receipt of passwords.
- Passwords shall never be stored on computer systems in an unprotected form.
- Default vendor passwords shall be replaced as soon as the installation of systems or software has been completed.

11.9.4 Monitoring of access/user activities

A set of controls shall be defined for controlling and monitoring user activities on the systems. The following shall, inter alia, be considered:

- Repeated failed login attempts shall be identified and investigated.
- Any blocked or suspended user ID (three or more consecutives failed attempts) shall be investigated to verify that the user is the authorized owner of the user ID and not an unauthorized person trying to discover passwords.
- Inactive users shall be monitored, and corrective action shall be taken after a predefined period of inactivity.
- Activity carried out by default users (e.g. guest, administrator, owner and root) shall be monitored daily.
- Access to critical accounts, log files, data files and databases shall be monitored.
- Periodically, logs shall be reviewed to monitor the activities of privileged users and failed access attempts.
- The department shall be prepared to react appropriately shall a breach of access such as an unauthorized intrusion be detected.
- Periodically, the department shall check for and remove or block redundant user IDs and accounts.
- The activities of the privileged or super user login account shall be closely monitored and reviewed by senior computer security management.
- Users' passwords shall be reviewed to ensure that an appropriate level of complexity is maintained.

12. ICT Patch Management Policy

12.1 Rationale

Vulnerability and patch management is an important part of keeping the components of the information technology infrastructure available to the end user. Without regular vulnerability testing and patching, the information technology infrastructure could fall foul of problems which are fixed by regularly updating the software, firmware and drivers. Poor patching may allow viruses and spyware to infect the network and allow security weaknesses to be exploited.

12.2 Purpose

This policy defines the procedures to be adopted for technical vulnerability and patch management.

12.3 Scope

This policy applies to all components of the information technology infrastructure which requires regular patches like:

- Operating systems
- Application Software
- Drivers
- Firmware
- Databases

All staff within the ICT unit shall understand and implement this policy. ICT staff is responsible for ensuring that the vulnerabilities within the ICT infrastructure are minimized and that patching of the infrastructure is kept up to date. All users shall have a role to play and a contribution to make by ensuring that patches are deployable to their equipment (i.e. log off and leave the computer on)

12.4 Risks

Without effective vulnerability and patch management, there is a risk of unavailability of the systems. This can be caused by viruses and malware exploiting systems or by out of date software and drivers making systems unstable.

12.5 Policy Statement

The department's ICT infrastructure shall be patched according to this policy to minimize vulnerabilities.

12.5.1 Up to date Inventory

- The ICT Department shall maintain an up to date inventory of the components within the department's ICT infrastructure.
- The software and hardware identified shall scan for vulnerabilities and patched according to this policy.

12.5.2 Vulnerability Scanning

The department network will shall be scanned at least three times in the financial year with technical vulnerability management tool being used.

12.5.3 Identifying Patches to be Applied

- The department's anti-virus server shall be configured to automatically download the latest virus and spyware definitions and push them to the servers, computers, tablets, etc. running in the network.
- Windows patch management tools shall be utilized to automatically download the latest Microsoft security patches. The patches shall be reviewed and applied as appropriate.
- Security weaknesses and software update notifications issued shall be monitored on a regular basis and any critical issues affecting the organization's ICT infrastructure shall be attacked upon immediately.
- Notifications of patches from application and database vendors shall be reviewed and the patches applied as appropriate. Where notifications are not automatically sent, the suppliers' website shall be reviewed on a regular basis.
- The websites of the suppliers of servers, PC's, tablets, printers, switches, routers and peripherals shall be reviewed to determine the availability of firmware patches.
- Missing patches identified as a result of vulnerability scanning shall be implemented as appropriate. Any weaknesses identified shall be rectified,

12.5.4 Types of Patches

The following patches shall be implemented on the different information infrastructure types

Type	Patch
Server / Computer	WSUS, BIOS, firmware, drivers
Operating System	WSUS, Service packs, patches, feature packs
Application Software	Service packs, patches, feature packs
Router and Switches	Firmware
Anti-Virus /Anti-Spyware	Data file/Virus definition update
Printers	Driver, firmware
Scanners	Driver, firmware

12.5.5 Patching Schedule

The department's ICT infrastructure shall be patched as and when the patches are available.

13. ICT Data Back-Up and Restoration Policy

13.1 Purpose

This section defines the standards and processes that shall be followed in LDoH for the backup of data and or Health Information System housed within the server rooms.

13.2 Scope

The policy applies to the active data stored on servers that are housed in the departmental server rooms. These systems are typically servers but are not necessarily limited to servers.

13.3 Policy Statement

- Backup
    - Data residing on servers which are owned and administered by LDoH shall be backed up daily.
- Restoration of Backed-up Files
    - All requests for file recoveries shall be made by completing and submitting the file recovery request form to the ICT service desk.
- Archiving of files
    - Files shall be archived immediately after the ICT unit has been notified that a user has officially left the department according to the rules laid down in the User Account Policy.

13.4 Enforcement

ICT unit is the custodian of this policy and shall enforce compliance with the requirements of this policy.

- The ability to restore data from backups shall be tested at least once per annum including actual restores.
- Data to be backed up include Application Data stored on the server hard drives.
- Systems to be backed up include but are not limited to:
    - Production Web server
    - Production Database server
    - Production Report server
- User account data associated with the file and mail servers shall be archived at least one month after the user has left the department.

13.5 Back-Up Tools

All database backups shall be done using RMAN or similar backup tool.

13.6 Schedule

All backups of the databases shall be scheduled to run between 20:00 and 06:00 daily.

13.7 Retention

Backups shall be retained for at least 7 days for all sites.

13.8 The Backup Process

- Backup scripts are automatically started at 00H00 daily.
- The database shall be backed up into a single file and shall be stored on the DB server disk.
- The file shall be compressed using the tar utility and shall be packaged with a date and timestamp.
- The tar file shall be copied over to the Report Server or alternative storage.

13.9 Offsite storage

- Data backups must be stored in two locations:

  (a) One on-site with current data in machine-readable format in the event that operating data is lost, damaged or corrupted; and

  (b) One off-site to additionally provide protection against loss to the primary site and on-site data.
- Minimum requirements are to store the weekly, monthly, quarterly and or yearly backup sets off site.
- Weekly, monthly and quarterly backups must be stored offsite for the entire duration of the retention period.

13.10 Responsibilities

- System Administrator/IT Technicians shall ensure essential business information is backed up at appropriate time intervals.
- Deputy Director: ICT Security shall ensure information is backed-up regularly as agreed upon with the IT Technicians.

14. ICT Wireless Access Policy

14.1 Rationale

The LDoH wireless network is designed to be a convenient supplement to the wired network for general functions including web browsing, e-mail, network filing and printing to public and private printers.

14.2 Purpose

Guide the deployment standard and integrity of wireless networking within LDoH to ensure reliable, compatible and secure operations. Protect the security of LDoH's information system and electronic communications by specifically prohibiting access to LDoH wireless networks through unsecured wireless communication devices.

14.3 Scope

The policy shall apply to staff employed by LDoH and consultants including anyone who shall be utilizing Wireless Local Area Network (WLAN) technologies at all physical locations that connect directly to LDoH's network backbone. This policy does not apply to cellular wireless technology or wireless devices networks that have no direct connectivity to LDoH's networks and where those devices do not interfere with LDoH wireless network.

14.4 Responsibilities

ICT unit is responsible for maintaining the availability of the department wireless network spectrum. The wireless network users utilizing this network shall adhere to the acceptable usage of wireless network and wireless network security. Wireless network shall be managed and controlled by ICT.

14.5 Policy Statements

14.5.1 Standard Technology for Wireless Networking

- The IEEE 802.11b standard for wireless LANs or any standard recommended by GITO shall be supported.
- All Health Clinics WLANs shall use Secure Socket Layer (SSL) for authentication for security, with exceptions for special circumstances approved by GITO.
- All Access Points and wireless client adapters on the LDoH WLAN shall use an SSID maintained by ICT or any recommended by GITO.
- Given the relatively weak security of WLANs, people shall be encouraged to use applications that support encryption such as SSL-based secure websites or Secure Shell (SSI-I) or others that may be recommended by GITO.
- The Authenticated Wireless Network currently employs WPA2 as ICTs primary authentication strategy. This provides secure authentication and over the air Advanced Encryption Standard (AES) encryption.

14.5.2 Wireless Network Security, Access and Guidelines

- Wireless networks shall be designed and deployed to avoid physical and logical interference between components of different network segments and other equipment
- As a minimum requirement, all wireless network access shall be through user-id and password authentication, their data shall be encrypted.
- All LDoH employees and contractors registered on the Active Directory shall automatically be granted access to log on (authenticate) to the wireless network using their normal login and password credentials.
- Devices that interfere with the wireless network may be subject to restriction or removal.
- Any wireless network in LDoH which poses a security threat may be disconnected from the campus backbone network. If a serious security breach is in process, the ICT may disconnect the LAN immediately.

In order to mitigate users' exposure to external threat, laptops and computers which are used to connect to wireless network shall:

- Utilize a personal firewall.
- Run anti-virus software with updated virus definition.
- Ensure that their operating system is fully patched and running the latest service packs.

14.5.3 Limited Support

- High band width applications like large file transfers, internet music and video download from the internet shall not be allowed.
- Media sharing or peer to peer with programs shall not be supported.

14.5.4 Unacceptable Misuse of Wireless Network

The LDoH Wireless Network shall not be used inappropriately; in particular, an employee shall not use the network to:

- Send, receive or make available any material that may be considered offensive, obscene or indecent.
- Send, receive or make available any material that may infringe copyright, e.g. unlicensed software, MP3 or other audio and video formats.
- Run peer-to-peer (P2P) file sharing software.
- Intercept or attempt to intercept other wireless transmissions for the purposes of eavesdropping.
- Access or run utilities or services which may negatively impact on the overall performance of the network or deny access to the network, e.g. RF jamming, Denial of Service (DOS).
- Harass, cause annoyance, nuisance or inconvenience to others.

- Access or attempt to access systems or resources to which an employee is not authorized
- Provide services which may interfere with normal network operation.
- Provide access to others, e.g. allowing a third party to use an employee's credentials to access the network.

14.5.5 Monitoring and Evaluation

Broadcast frequencies and the usage of wireless network shall be monitored and evaluated by ICT to avoid unauthorized of unacceptable misuse of wireless network and interceptions that shall be done by other wireless transmissions for the purposes of eavesdropping.

14.5.6 Training and Awareness

Staff shall (including contractors/temporary employees and interns) be made aware of all policies applicable to them and the risks of non-compliance. The ICT unit shall provide training and conduct awareness to all computer users of different systems to ensure adherence to the policy.

14.5.7 Breaches of Security

The ICT Security team shall report all instances of breach of security, or failure to comply with security measures constituting a security risk as soon as possible to the GITO. Where official encryption is concerned, a security breach shall also be reported to the State Security Agency (SSA). Breaches of Security shall at all-time be dealt with using the highest degree of confidentiality.

14.5.8 Non-compliance and Policy violation

Computer users who do not comply with any of the policy requirements may be subject to disciplinary action. This may also result in restriction of access to LDoH's computer systems.

15. ICT Firewall Management Policy

15.1 Introduction

Firewalls are an essential component of information systems security infrastructure. Firewalls are defined as security systems that control and restrict both Internet connectivity and Internet services. Firewalls establish a parameter where access controls are enforced.

15.2 Purpose

To define standards for provisioning security devices owned and/or operated by LDoH and to prevent exploitation of insecure services, restrict inbound/outbound traffic from unregistered devices, control inbound/outbound access to/from specific services or devices and monitor traffic volumes.

15.3 Scope

This policy defines the essential rules regarding the management and maintenance of Firewall at LDoH and the policy will apply to all users that use computers and the network of LDoH.

15.4 Policy statement

LDoH perimeter firewalls are a key component of the overall departmental Network Security Architecture. This policy governs how the perimeter Firewalls will filter Internet traffic to mitigate risks and possible losses associated with security threats to the networks and information systems.

15.5 Requirements

- The Firewall system shall control all traffic entering and leaving the LDoH Internal network.
- LDoH Firewall shall block all unknown/unsolicited incoming and outgoing traffic by default.
- Only authorized incoming and outgoing traffic shall be allowed to pass through the firewall.
- Traffic with invalid source or destination addresses shall always be blocked.
- Traffic with an invalid source or destination address shall be blocked.
- Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an “internal” address) shall be blocked at the network perimeter.
- Outbound traffic with invalid source addresses shall be blocked.
- Incoming traffic with a destination address of the firewall itself shall be blocked unless the firewall is offering services for incoming traffic that require direct connections.

15.6 Operations

- Only Firewall system administrators shall be permitted to logon to Firewall hosts. Access to firewall hosts shall be tightly controlled. Only Firewall system administrators can have user accounts on Firewall hosts. Firewall system administrators shall have personal accounts; i.e. no group logins are allowed.

- All changes to Firewall access rules shall be made through a single approved interface. The firewall shall have a trusted path for its management e.g. a logically secure access to the Firewall management process with a password-based identification and authentication system.

- Only personnel with the appropriate authorization shall make changes to the Firewall access rules, software, hardware or configuration. All changes shall be as a result of a request recorded in a Change Management Form although emergency modifications can be requested over the phone, with a follow up email and change request. Only authorized personnel must be able to implement the changes and an audit log must be retained.

- Logging and audit facilities provided by the Firewall system shall be fully utilized. All significant traffic through the Firewall shall be logged. The Firewall shall provide sufficient audit capacity to detect breaches of the Firewall's security and attempted network intrusions. Firewall System Administrators shall examine logs on a regular basis and set up mechanisms to respond to alarms.

15.7 Configuration

- The perimeter Firewall system shall be configured to deny any service unless it is expressly permitted. If there are no rules defined for the department network address, then traffic to or from that address shall be denied. Access to the department network shall be blocked during the start-up procedure of the Firewall.

- The Firewall operating system shall be configured for maximum security. The underlying operating system of Firewall hosts shall be configured for maximum security, including the disabling of any unused services.

- The Firewall product suite shall reside on dedicated hardware. Applications that could interfere with, and thus compromise, the security and effectiveness of the Firewall products, shall not be allowed to run on the host machine.

- The initial build and configuration of the Firewall shall be fully documented. This provides a baseline description of the Firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

- Security shall not be compromised by the failure of any Firewall component. If any component of the Firewall fails, the default response will be to immediately prevent any further access, both outbound as well as inbound. A Firewall component is any piece of hardware or software that is an integral part of the Firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons

- e.g. bad maintenance of the rules database on the Firewall or software which is incorrectly installed or upgraded.

- There shall be regular reviews to validate the Firewall system meets the needs of the department regarding information security. The configuration of the Firewalls shall be regularly checked to ensure they still match the business requirements regarding the security. The Firewall must also be regularly tested for vulnerabilities. Applications on internal hosts that handle incoming services will need to be checked for known vulnerabilities.

15.8 Audit and Compliance

- Regular testing of the Firewall shall be carried out. The Firewall shall be regularly tested for configuration errors that may represent a weakness that can be exploited by those with hostile intent.
- Consistency of the Firewall rule set.
- Secure base system implementation.
- The Firewall system shall have an alarm capability and supporting procedures. When an agreed specified event occurs, an alarm shall be sent to the security team. Documented procedures shall exist to permit an efficient response to such Firewall security alarms and incidents
- There shall be an active auditing/logging regime to permit analysis of Firewall activity both during and after a security event. An audit trail is vital in determining if there are attempts to circumvent the Firewall security. Audit trails must be protected against loss or unauthorized modification. The Firewall system must be able to provide logging of specific (or all) traffic when suspicious activity is detected.

15.9 Responsibilities

IT Unit will be the sole responsible entity for putting in place firewalls and the management thereof.

15.10 Change control

All changes in the Firewall configuration shall go through change control. When rules are introduced there should be a well-defined method for documenting these and in the case of temporary rules, the removal date for the rule should be added in a comment field. All changes shall be as a result of a request recorded in a Change Management Form.

15.11 Monitor stability

A Firewall is like any other infrastructure component and should be managed as such. It should be monitored for availability to ensure maximum uptime. If a Firewall isn't stable, people will find ways of avoiding the Firewall that leads to a low level of security.

15.12 Enforcement

IT Unit is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

16. Virtual Meeting Policy

16.1 Purpose

The Limpopo Department of Health (LDoH) encourages virtual meetings if face-to-face meetings are not necessary or possible. This policy provides guidance when officials hold and participate in virtual meetings.

16.2 Definition

Virtual meeting: is real-time interactions that take place over the Internet using integrated audio and video, chat tools, and application sharing. This web-based meeting allows participants to see and/or hear each other, talk in real time and may make presentations with visual aids such as charts and graphs.

16.3 Legal Framework

This policy has taken into consideration all relevant legislation and statutory guidance including, but not limited to, the following;

- Electronic Communications Act, 2005
- Public Service Act, 1994
- National Archives and Records Service of South Africa Act 43 of 1996
- Protection of Personal Information Act, 2013

16.4 Related Documents/Policies

- Information and Communication Technology (ICT) Policy
- Records Management Policy
- Minimum Information Security Standards (MISS)
- Code of Conduct for Public Service

16.5 Scope

This document seeks to regulate virtual meeting procedure in relation to technology aspects and does not seek to define meeting procedures. Normal meeting procedure is still applicable. This policy applies to all officials in the department who initiate or participate in the virtual meeting.

16.6 Roles and Responsibilities

Role	Responsibility
Initiator (PA or Office Admin)	• Notifying participants in advance that the meetings will be conducted virtually • Providing meeting details, i.e. link, ID and or password

	• Recording the detail of the virtual meeting within written minutes and/or audio • Share or upload meeting document • Download the electronic attendance register
Chairperson	• Ensuring all participants are aware of the procedures outlined in this policy • Deciding whether a recording is appropriate during the virtual meeting and notifying participants that a recording is taking place, prior to the meeting • Requesting participants to activate cameras at any given time
Participants	• Be aware of, and act in accordance with, the procedures outlined in this policy • Provide changes to be considered during the review of the Policy • Alert relevant officials when the policy becomes out of date or obsolete
Custodian of the Policy	• Be able to interpret and explain policy content • Provide oversight to ensure policy content is relevant and accurate • Review the policy and make recommendation for approval • Ensure that the final approved policy document has been communicated to all officials
Employer	• Provide tools of trade (i.e. devices and connectivity) to ensure that employees can participate in the virtual meetings

16.7 Virtual Meeting Procedure

Prior the meeting

16.7.1 Scheduling of meeting

Scheduling a virtual meeting should not differ much with scheduling the face-to-face meeting. Schedule each meeting separately to ensure unique identity of the meeting as there may be chat messages and shared documents specific to that meeting. The meeting initiator should;

- Use Microsoft Teams to schedule a virtual meeting as the Department has invested in this tool (use of any other tools is discouraged as ICT does not have control of these tools),
- Ensure that the meeting link or details have reached all the participants and

- All documents to be used in the meeting are in his/her possession to avoid delays due to multiple people sharing the screen.

16.7.2 Connecting to the meeting

- Any device with internet access can be used to connect to the virtual meeting.
- It is the responsibility of the participants to ensure that he/she can connect to the meeting. Hence participants are advised to test the meeting link in advance to ensure that assistance provided before the meeting.
- All problems should be directed to the local ICT technician or alternatively call ICT Helpdesk at 015 293 6196/6096.
- Participants should be connected to the meeting at least 5 minutes before the meeting starts.

During the meeting

16.7.3 Attendance

- Full name and surname should be used when participants join the meeting using a browser so that they can be easily recognized.
- The meeting initiator should download the attendants list twice, in the first and last 10 minutes of the meeting. This list will be used as attendance register or complement the register that the secretary may develop.
- In case where more than one participant is using the same device, their names should be communicated to the chairperson verbally.
- The chairperson shall instruct participants to activate cameras anytime during the meeting

16.7.4 Recording

- Recording of the meeting on any device or program by the secretariat, shall be done if it is to assist the secretariat to write minutes accurately.
- Participants shall not record the meeting discussions.

16.7.5 Participation

Participants shall,

- Adhere to the meeting etiquette as outlined in Annexure A.
- Use a raise hand icon or chat platform to be recognized by the Chairperson should you want to speak or vote.
- Identify themselves before speaking in order to assist the secretary in recording the minutes.
- Notify the Chairperson of their departure (either temporary or permanent) from the meeting before absenting themselves. This can be done through a message in the chat area or any other message that will reach the chairperson.

16.7.6 Retention of the meeting recording

The creation, storage, retention and disposal of recordings shall be in line with the requirements of the National Archives and Records Service of South Africa Act 43 of 1996 and the supporting Records Management Policy.

Post the Meeting

The secretariat shall ensure that all participants have left the meeting to ensure that recording is stopped on time.

16.8 Data Efficiency

Keep your camera disabled especially when you are connected through limited data network unless instructed so by the chairperson.

17. Inception date

This policy shall be effective from the date of approval by the Head of Department or delegated official.

18. Review

This policy shall be reviewed every three years or earlier as directed by the office of GITO.

19. Enquiries

All enquiries on this policy should be made to the following office, Office of the GITO, Limpopo Department of Health, Office number 106, Whitoc building Helpdesk@dhsd.limpopo.gov.za, 015 293 6463.

Annexure A: Virtual Meeting Etiquette

1. Treat a virtual meeting just as you would if you were in a face-to-face meeting.
2. Dress as if you are in the office, or at least appropriately. You never know if you'll need to get up suddenly or your camera falls off the monitor.
3. Setup:
    a. Make sure the area behind you is organized. Get rid of distracting artwork on your walls, which can prevent your team from focusing on what you are saying.
    b. Adjust your camera before the meeting. Position it at eye-level and on the monitor, you are using for the conference. It is unflattering when the camera is either too low (double chin alert!) or too high, and when you are looking at another screen while on the call.
    c. Make sure you are in a quiet area. Limit the background noise (e.g., kids, pets, etc.)
4. Joining:
    a. Join the meeting on time or a few minutes early.
    b. If joining after the meeting has started, wait for the conference leader to ask who joined. This
    c. will prevent you from possibly interrupting the presenter and further disrupting the meeting.
5. Audio:
    a. Keep your microphone on mute if you are not actively engaged in a conversation.
    b. Be aware of your microphone settings, as you do not want to start a monologue while on mute.
6. Video:
    a. Limit your movement when you speak and look into the camera. This gives a better impression than a side view
    b. Avoid excessive use of your hands or off-camera motion, and don't put your face too close to the camera.
    c. Limit your getting up and walking around while showing video
    d. When presenting look at your camera as if you were looking at your audience in a room.
7. Behaviour:
        a. Avoid multitasking (checking email, eating, drinking, etc.), and give your full attention throughout the meeting and encourage participants to do the same.

b. Mute mobile phones turn off notification sounds and minimize other applications like email or Jabber. Your colleagues can easily tell when you are not completely involved.

c. Don’t have side conversations. If you wouldn’t do it in an in-person meeting, then you probably shouldn’t do it in a virtual one. It is distracting even if you are on mute.

d. Never place the meeting on hold, simply drop and re-join when you can.

8. Speaking

    a. Identify yourself before you speak. Otherwise it’s difficult to know who is speaking.

    b. When speaking, keep your points clear and concise.

    c. Don’t interrupt other speakers while they are presenting. If you have a question that cannot wait, type it in the chat window so that it can be addressed later.