Republic of Malawi

PUBLIC SERVICE

ICT STANDARDS

January 2014

Table of Contents

FOREWORD

The Government of the Republic of Malawi recognizes that the presence of a capable, effective, and forward-looking Public Service that will be able to implement the Government's development policies and deliver services in an efficient and timely manner, is a pre-requisite for fulfilling the good governance goals articulated in Vision 2020 and the Malawi Growth and Development Strategy (MGDS).

The Malawi Growth and Development Strategy have included provision of electronic services by the public service as one of the indicators for the growth of the ICT industry and overall economic growth of the country. The National ICT Policy has lined up strategies for implementing the policies under the various focus areas which will see ICT being mainstreamed in all sectors of the economy. The Public Service ICT Standards focus on mainstreaming of ICT in the public service to ensure that government realises the potential of ICT in the efficient management of the public service and improvement of delivery of services to the general public. The standards have been developed for specific critical areas of the Public Service.

Provision of some of the public electronic services will require regulations and legislation, which have been provided for through the E-Transactions and Management Act that is expected to be enacted within the first year of implementation of the National ICT Policy.

I would like to thank the World Bank for providing financial support through the Regional Communications Infrastructure Programme managed by the Privatisation Commission that facilitated the review of the Civil Service ICT Policy and the developing of the Public Service ICT Standards. I would also like to thank Leading Associates for their expertise in carrying out the review of the Civil Service ICT Policy and drafting a revised Public Service ICT Standards.

Further appreciation goes to Principal Secretaries and their officers who participated in the development of these Standards.

It is my expectation that all Ministries, Departments and Government agencies will adhere to the Standards set here forthwith.

Signed

Hawa O. Ndilowe (Mrs)
CHIEF SECRETARY TO GOVERNMENT

PREFACE

Government of Malawi has developed the Public Service ICT Standards in order to ensure a systematic approach to ICT development, management and utilization in the public service.

This document was formulated with financial resources from World Bank through Regional Communications Infrastructure Programme (RCIP) from years 2011 to 2013. A consulting firm, Leading Associates, coordinated the development process. The process involved in-depth consultations conducted with stakeholders throughout Malawi Public Service.

I trust that utilisation of these standards will assist in improving the efficiency and effectiveness of ICTs as a crosscutting tool to the delivery of public service.

Olive T. Chikankheni
SECRETARY FOR E-GOVERNMENT

LIST OF ACRONYMS AND ABBREVIATIONS

CD / CDROM	Compact Disk / Compact Disk Read Only Memory
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
CTO	Chief Technical Officer
DISTMS	Department of Information Systems and Technology Management Services
DVD	Digital Video Disk
GOM	Government of Malawi
GWAN	Government Wide Area Network
ICT	Information and Communication Technology
ISP	Internet Service Provider
IT	Information Technology
ITIL	IT Infrastructure Library
ITSM	IT Service Management
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Standards Organization
LAN	Local Area Network
MDA	Ministry, Department and Agency of government
MGDS	Malawi Growth and Development Strategy
MISTMS	Management Information System and Technology Management Services
MOF	Ministry of Finance
MPSR	Malawi Public Service Regulations
NGO	Non-Governmental Organization
ORMP	Operational and Resource Management Plan
PC	Personal Computer
PRINCE2	Projects in Controlled Environments
SLA	Service Level Agreement
USB	Universal Service Bus
Val IT	IT Value Delivery

CHAPTER 1

INTRODUCTION

1.1. Compilation of ICT Standards

This document is a compilation of ICT Standards that have to be adhered to in the development and utilization of ICT in Malawi Public Service. This document contains the following Standards:-

1. Acceptable Use of ICT Facilities in the Public Service;
2. Electronic Records Management;
3. Information Asset Classification and Control;
4. Information Systems Security Management;
5. Data Back-up;
6. ICT Audit;
7. ICT Project Management;
8. Systems Development;
9. e-Waste Management;
10. Strategic and Operational Planning; and
11. Tele-centers Management.

CHAPTER 2

SUMMARY OF THE STANDARDS

2.1. Acceptable use of ICT Facilities in the Public Service

This standard defines the control and protective measures for the use of ICT Equipment, Internet, E-mail, and other ICT resources to ensure that they are appropriately used for the purposes for which they were acquired. Information resources, all types of application software, hardware, network facilities, and similar devices, must be used appropriately, responsibly and with accountability.

2.2. Electronic Records Management

This Standard outlines the standards, including objectives, scope and structure, of the Document Management Process.

Furthermore, it identifies the various stages of a document life cycle that may apply to these documents and the standards and conventions that should be considered when creating or maintaining an electronic document intended for use or reference by more than one person within or outside the organization..

The security level of access to any document is to be determined prior to the publishing process. The intention is to provide a framework for the development and maintenance of electronic documents that are consistent and present a professional image appropriate to the intended audience.

The Standard is divided into three separate sections to enable the various ICT stakeholders to quickly go to the relevant section to find the information necessary to understand and comply with the requirements.

2.3. Information Asset Classification and Control

The Standard defines guidelines for the classification and management of sensitive information that is handled, created, received and/or destroyed by an organization in accordance with its sensitivity, confidentiality of content and business importance, based upon legislative, regulatory and contractual requirements.

2.4. Information System Security Management

The standard details the processes in place to ensure that ICT systems of an organization are maintained and operated in a secure manner.

2.5. Data Back-Up

The standard provides directions and guidance on the data back-up management (including restoration) performed by the ICT Staff working in an organization The standard does not include provision for hand-held devices.

2.6. ICT Audit

The Standard details the processes put in place to carry out ICT Audit. In line with rapid advancement of technology most organisations have become increasingly reliant on computerised information systems to deliver public services and carry out their daily operations. As a consequence, the reliability, integrity and availability of computerised data and of the systems that process, maintain and report these data are a major concern to audit. ICT Auditors examine the adequacy of controls in information systems and related operations to ensure system effectiveness.

ICT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organisational goals to be achieved effectively, and uses resources efficiently.

ICT auditing is a branch of general auditing concerned with governance (control) of information and communications technologies (computers).

2.7. ICT Project Management

The standard provides an overview of the essential components of the project management methodology used within an organization. The Standard includes the 'what', 'when' and 'why' of project management methodology. Examples of 'how' can be found in supporting procedures and forms. As a methodology, this Standard provides a structured approach to managing projects with ICT components.

2.8. System Development

The Standard defines what controls will be implemented by an organization in relation to System Development and Maintenance. This standard is consistent with, and should be read in conjunction with the Information Systems Security Standard. The Standard interprets current industry standards and recommends an application development standard for adoption in an organization for the software/application development lifecycle, consistent with the organization's enterprise architecture standards (in particular, compliance with the enterprise architecture checklist), principles, and best practices.

2.9. e-Waste Management

The Standard defines the obligations and processes to ensure that an organization disposes of unwanted and obsolete ICT electronic equipment and waste with due regard to environmental and security factors.

2.10. Strategic and Operational Planning

This Standard details the processes in place to ensure that ICT strategic and operational planning is aligned to an organization's business needs. The standard is

intended to identify the various processes and activities performed within an organization that influence the allocation of ICT resources towards ensuring projects and activities are aligned to achieving the business requirements of the organization..

2.11. Tele-centers Management

This Standard has outlined best practices in investing in and operating a tele-center.

CHAPTER 3

THE STANDARDS

3.1. Acceptable use of ICT facilities in the public service

3.1.1. General Directives

GOM information resources, all types of application software, hardware, network facilities, and similar devices, must be used appropriately, responsibly and with accountability. Any damage to ICT properties or corruption of software and data as a result of the user's negligence shall be dealt with accordingly upon validation of fault. When using Government ICT resources the following requirements must be adhered to:

- All concerned shall take appropriate action with due diligence to comply with hardware warranty or conditions of use, software license agreements and respect of the rights of other authorized users of the facility.
- Users shall be accountable for their ICT facility personal access accounts and the personal access accounts of others. Each user is obliged to report unauthorized access or transactions.
- Each user is accountable for his/her own work or data, and accountable for the work or data of other users of the ICT facility.
- Users shall use only the machines or component ICT facilities for which they are authorized.
- Access accounts must be used for intended purposes only. Government ICT facility shall be used for purposes of GOM related work only.
- All users must cooperate with the systems administrator. The systems administrator is authorized and may access the user's work or data if deemed necessary to maintain a secure environment and ensure effective and efficient use of the ICT facility.
- All users are directed to report any illegal activity and wrong-doing to Responsible Business Unit Managers and Organisation responsible for ICT implementation or regulation in Malawi ICT Common Services. In the event of an official investigation, all users are mandated to cooperate to the fullest extent of their capacity and authorization.

The organisation responsible for ICT implementation in Malawi shall ensure proper communication and documentation of Government expectations for handling sensitive data.

3.1.2. Use of ICT Hardware and Software Resources

3.1.2.1 Hardware Management

Any installation or deployment, configuration and maintenance of computer equipment are the responsibility of the organisation responsible for ICT implementation in Malawi. Maintenance action or procedures shall comply with enforced warranty or related maintenance agreements.

3.1.2.2 Hardware Documentation

The organisation responsible for ICT implementation in Malawi shall maintain a register (inventory) of the Government's ICT equipment. This includes custodian list, Local and Wide Area Network setup/diagram, systems specifications, and configurations. A periodic inspection and update of register shall be conducted by the organisation responsible for ICT implementation in Malawi. The inventory shall include IT special projects or any IT related undertaking of the Government.

3.1.2.3 Hardware Protection and Insurance

Organisation responsible for ICT implementation in Malawi will liaise with concerned office to ensure adequate insurance coverage for ICT equipment/facility. Likewise, organisation responsible for ICT implementation in Malawi shall ensure that adequate facilities which are critical to the physical protection of the device or its environment are installed to prevent or minimise the effect of fire, flooding, and similar physical threat. Organisation responsible for ICT implementation in Malawi will ensure that staff are aware of restrictions and limitations.

3.1.2.4 Procurement

Procurement of ICT equipment in amounts in excess of K10million is subject to the approval of the ICT Steering Committee. Any ICT procurement valued at less than K10million, approved by Senior Management, shall require review of the organisation responsible for ICT implementation in Malawi. Requirements for new hardware and software should be discussed in advance with the organisation responsible for ICT implementation in Malawi to assess the detailed specification of the equipment.

And a written technical advice from the organisation responsible for ICT implementation in Malawi to the procuring entity shall be part of the presentations to the ICT Steering Committee.

3.1.2.5 Movement of ICT Equipment

Any movement of ICT equipment or transfer of custody shall be duly coordinated with the organisation responsible for ICT implementation in Malawi for necessary processing (update of register and insurance policy). Movement or transfer shall comply with requirements on disposal, servicing, transfer of ICT equipment. Movement or transfer shall not be left to any individual, or private sector organization or person.

3.1.2.6 Use of Portable Equipment

Laptops, multi-media display, or any portable media, or other ICT equipment used outside of the Government premises for official business shall be logged in/out for proper tracking of equipment movement. The security and safekeeping of portable and other equipment used outside of Government premises is the responsibility of the staff using it.

3.1.2.7 Designation or Sharing of Portable Equipment

Distribution or assignment of laptops or notebook PC or any similar portable computing device should follow "Function vs. Equipment Assessment" result as presented in the Operational and Strategic Planning section of this standard. Designation of a portable computing device to a specific employee position shall follow the general rules on care and manufacturer instructions. Portable computing devices designated to be common (shared) shall be managed solely by organisation responsible for ICT implementation in Malawi.

Portable Device Request Procedure:

- Fill out form for request
- Submit to organisation responsible for ICT implementation in Malawi for immediate processing
- Organisation responsible for ICT implementation in Malawi facilitates availability of unit upon approval
- Organisation responsible for ICT implementation in Malawi releases the unit to the requesting party

Note: The requesting party should not be the one to get the device from previous user.

3.1.2.8 Software Installation

The organisation responsible for ICT implementation in Malawi is responsible for all software installation, deployment and configuration on all Government-owned ICT

equipment. Unauthorized software installed will be deleted without need to notify the user.

3.1.2.9 Loss or Damage to ICT Equipment

In the event of loss or damage to any ICT equipment the rules and regulations, as outlined in the MPSR, will be followed.

3.1.2.10 Portable Storage Devices

Government provided portable external storage devices should be given appropriate care by the employee in custody as described in the manufacturer's instruction for care.

Any personal portable external storage device upon processing (registration, scanning, sanitizing, etc.) of the organisation responsible for ICT implementation in Malawi and approved for use within the Government's ICT Facility shall be the responsibility of the owner of the device.

Loss or damage of said device or data stored therein shall be the responsibility of the owner or any loss or damage caused by the device to any Government/Project owned ICT equipment shall be the liability of the owner of the personal device.

3.1.2.11 Schedule of User Performed Hardware System Maintenance

It is mandatory for all employees with designated PC system or with personal computing/storage device to schedule and perform the following maintenance at least once per week, as appropriate:

- scan and clean systems from computer viruses (full scan)
- clean the registry
- check hard disks for errors
- defragment the hard drive

3.1.2.12 ICT Equipment Care

All employees shall be responsible for the proper usage, care and cleanliness of the ICT equipment they use. Responsible Business Unit Managers shall ensure that their staff maintains the cleanliness of their machines. Only approved and authorized cleaning solutions and materials shall be allowed for use.

3.1.2.13 Safety Precautions

Health and safety with regard to use of computer equipment and computer workstations should be managed within the context of the general and specific Health & Safety policies and procedures of the Government.

3.1.2.14 Cables, Links, Wire etc

Only power cables and accessories and the like that come with ICT equipment and portable devices like multimedia projectors, should be used. Any alternate use of cables, links, wire, etc. shall require authorization from the organisation responsible for ICT implementation in Malawi .

3.1.2.15 Non Government Users

Visitors, guests or even government employees from other agencies are prohibited from using any ICT facility owned by the Government unless given explicit permission by the supervisor or senior officer of the unit, section or office visited.

3.1.2.16 Service Requirements

Problems with hardware should be reported to the organisation responsible for ICT implementation in Malawi and ICT Unit within an MDA. Servicing of any ICT equipment should not contravene with any related agreement, laws on Intellectual Property, license agreement etc. Outsourced servicing of ICT equipment should conform to this standard document.

3.1.2.17 Software

All employees are instructed to protect software license agreements as defined in the 'software licenses' section in this document.

3.1.2.18 Miscellaneous Devices and Accessories

All ICT devices and accessories attached to any ICT equipment, systems or network such as Biometric Scanners, PC Desktop Camera, Wireless USB modem, Scanners, etc. shall be given appropriate care. Loss or damage due to misuse or intentional cause is considered a grave offense.

3.1.3. Security

3.1.3.1 New Appointments

Responsible Business Unit Managers should notify the organisation responsible for ICT implementation in Malawi to allow the creation or deletion of network and e-mail accounts and PC system permissions for new staff and for staff leaving the unit.

3.1.3.2 User responsibility

Users should change their access codes when prompted by the system in the case of networked machines or on a regular basis for standalone machines.

3.1.3.3 Protection against viruses

Viruses or such worms are detrimental to performance of an electronic system, and they must be prevented and eradicated.

Users, whether standalone or networked, should clean viruses on their computers on daily basis.

The organisation responsible for ICT implementation in Malawi shall ensure that Government has antivirus software with which users can ensure that their systems are virus free.

The organisation responsible for ICT implementation in Malawi shall configure antivirus on the Government Wide Area Network servers and clients such that cleaning of viruses on the network is automatic.

MDAs shall ensure that they have a standalone computer on which removable data storage mediums can be cleaned off viruses before use of the removable data storage mediums into other computers. Otherwise, use of removable data storage mediums from one computer to another is prohibited.

The organisation responsible for ICT implementation in Malawi will provide facility, assistance and training when required.

3.1.4. Use of e-Mail

3.1.4.1 General Directives on Use of Government provided e-Mail System:

Electronic mail or "e-mail" systems are important alternative means of communication. In certain business functions, e-mail is preferred more than other conventional methods of communications. When using the Government e-mail system the following general considerations apply:

- Minimize Messages - For Government provided e-mail accounts, employees should minimize the number of messages in their e-mail in-box to ensure efficient function of the e-mail system.
- Maintenance of Messages - Garbage messages should be deleted regularly. Folders should be set up and messages filed accordingly.
- Archiving and storing - Employees should utilize the archiving facility within the e-mail system in accordance with allowed storage capacity and guidelines.
- Accounts and passwords - A register of e-mail accounts and passwords updated regularly shall be maintained by organisation responsible for ICT implementation in Malawi.
- Password and account expiration - It is mandatory to change e-mail passwords every 30 days or as necessary. The e-mail accounts of employees

separated from the Government shall be processed and deleted upon approval of Senior Management.

- Password security – Users should safeguard their electronic identity. Sharing of password, for example, is prohibited.

3.1.4.2 Examination of e-Mail Use

The Government retains the right to access and view all e-mails sent and received by the Government e-mail system. All employees whether regular, contractual, or circumstantial are required to give consent to the examination of the use and content of their e-mail accounts with due approval of Responsible Business Unit Managers and in strict observance of personal privacy. This right is exercised solely through organisation responsible for ICT implementation in Malawi upon official written instruction of a member of Senior Management.

3.1.4.3 Limitations on Personal Use

Very limited use of Government provided e-mail system for personal use is permitted. However, Responsible Business Unit Managers should ensure that there is no abuse of this privilege. Personal use of Government e-Mail account may only occur under the following circumstances:

- Use and access only during work breaks or after office hours,
- Personal use of e-mail should not interfere with work.
- Personal e-mails must adhere to the guidelines in this standard.
- Personal e-mails must be kept in a separate folder, named 'Private'. The e-mails in this folder must be deleted weekly so as not to clog up the system.
- The forwarding of chain letters, junk mail, jokes and executable files is strictly prohibited.
- Mass mailing is strictly prohibited.
- All messages distributed via the Government e-mail system, even personal e-mails, are Government property.

3.1.4.4 Group Sending of e-mail

Group/List sending of e-mails should be used appropriately. Spamming is prohibited. E-mail to all staff (broadcast) concerning official business function should be used only when appropriate.

3.1.4.5 Confidential Materials

Official and confidential materials sent through e-mail should be encrypted. The organisation responsible for ICT implementation in Malawi will provide encryption tools.

3.1.4.6 Non-Government e-mail Systems

For Civil/commercial provided e-mail systems, employees should seek approval from Senior Management, through organisation responsible for ICT implementation in Malawi before accessing or using any said accounts on any Government provided ICT equipment. At a minimum, only the following conditions shall be the basis for approval:

- If the Civil/commercial account will be used for official business function only.
- If the employee seeking approval, as a condition, shall permit the Government to access and review the account as required.

3.1.4.7 E-mail Access Using Government ICT Resources

Government IT resources used to operate Government provided e-mail service or Civil/commercial operated e-mail services must not be used for the following:

- Political, commercial and personal purposes not related to the Government.
- Illegal, pornographic, or cause to harm any entity, or any inappropriate material.
- Sending or forwarding e-mails containing libellous, defamatory, offensive, racist or obscene remarks, or any similar nature.
- Forwarding messages without acquiring permission from the sender.
- Sending/Forwarding unsolicited e-mail messages.
- Forging or attempting to forge e-mail messages.
- Sending e-mail messages using another person's e-mail account without permission from the originator.
- Copying messages or attachments belonging to another user without permission from the originator.
- Disguising or attempting to disguise one's identity when sending e-mail. Note: If you receive an e-mail of this nature, you must promptly notify the network administrator.

3.1.4.8 Signature

A Signature must be included on all emails that include your name, job title and agency name. A disclaimer will be added underneath your signature (see Disclaimer)

3.1.4.9 Disclaimer

The following disclaimer will be added to each outgoing e-mail:

'This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this

e-mail in error please notify the system manager. Please note that views or opinions presented in this e-mail are solely those of the author and do not necessarily represent those of the Government. Finally, the recipient should check this e-mail and any attachments for the presence of viruses. The Government accepts no liability for any damage caused by any virus transmitted by this e-mail.'

3.1.5. Internet Use

3.1.5.1 Purpose of Use

Access to the Internet is provided for official purposes; therefore, any act relative to the use of Government provided internet access should be for official purpose only.

3.1.5.2 Examination or Monitoring of Internet Use

The Government retains the right to monitor the Internet usage of employees. All employees, whether regular, contractual, or circumstantial, shall give consent to the examination of the use and content of their internet activity/history as required, with due approval of Responsible Business Unit Managers and in strict observance of personal privacy. This right is exercised solely through organisation responsible for ICT implementation in Malawi and, where relating to a specific staff, only on written instruction from an authorized official and related to a legitimate government function.

3.1.5.3 Limitation on Website Browsing

Access or any act similar to viewing pornographic, obscene, violent, gambling, illegal or other similar web sites using Government provided internet facility is prohibited. Government employees are duty-bound to report such abuse by co-employees. This standard also applies to access using non-Government provided internet but within the premises of the Government and using or not using any Government provided ICT resources.

3.1.5.4 On-line Communities, Subscriptions and other Web 2.0 Services

It is prohibited to operate, participate in, contribute to on-line communities or subscribe to other similar on-line groups over the internet while in the workplace unless permission is officially granted by Senior Management. Below are conditions for approving permission:

- On-line Communities/Subscription is to support or improve work related tasks
- On-line Communities/Subscription sites operate in secure environment and this should be verified by organisation responsible for ICT implementation in Malawi.
- On-line Communities/Subscription does not entail cost to the Government.

- Participation in On-line Communities/Subscription does not violate Government ICT policy, rules and regulations and any local and national law.

3.1.5.5 Programs and Executable Files

Any program or executable file, including screensavers, or any similar format when using Government provided machine through Government provided internet access are not to be downloaded. Any required program or application required in performance of an official function shall be sourced through organisation responsible for ICT implementation in Malawi. This is to prevent indiscriminate downloading and installation of programs or applications that may slow down ICT resources performance and at worst, threaten security of facility.

3.1.5.6 File Download

Downloading of movies, video, music, images and similar file formats not related to any official or legitimate government function is strictly prohibited. Scanning for virus is a mandatory pre-requisite before opening any file or program downloaded through the internet.

3.1.5.6 Secure Internet Access

All employees who have access to the internet should ensure the use of said facility does not compromise stability and security of the ICT facility environment. Should anyone accidentally/mistakenly allow this to happen, the systems administrator must be notified immediately.

3.1.6. Network Use

3.1.6.1 General Network Access

Network facility and bandwidth is limited, therefore access and use of the facility is managed according to priorities and importance. Below are limitations to the use;

- Access shall be on a 'work process reserved' basis.
- Organisation responsible for ICT implementation in Malawi does not guarantee Internet connection reliability and consistency, only the reliability of the GWAN (Organisation responsible for ICT implementation or regulation in Malawi controls the GWAN, but Internet service is provided by external ISPs).

3.1.6.2 Network Management:

Network installation, administration and maintenance within the Government are the responsibility of qualified and authorized organisation responsible for ICT implementation or regulation in Malawi Staff only. Access to, and management of the Network Servers are restricted to authorized staff.

3.1.6.3 Network Access Information

Disclosing any assigned IP address, Systems Administration password and any similar key that may compromise access, security of network and data is prohibited. Any knowledge of such disclosure should be reported to organisation responsible for ICT implementation in Malawi .

3.1.6.4 Tampering and Unauthorized Access

Unauthorized connection physical or virtual to any framework or device; or tampering of network cables or any similar device within the Government is prohibited and will constitute grave offense. Any knowledge of such activity should be reported to organisation responsible for ICT implementation in Malawi.

3.1.6.5 Jeopardizing Network Integrity

Any action that may damage, destroy, and negatively affect performance or any similar act that may intentionally or unintentionally jeopardize any network device or facility is prohibited. Any cost incurred out of such recklessness or negligence shall be borne by the person liable.

3.1.7. Use of Wireless Communications

3.1.7.1 Unauthorized Installation of Wireless Hardware

Connecting or attempting to connect a wireless device to the Government Internet or LAN wireless service is prohibited unless approved by organisation responsible for ICT implementation in Malawi.

3.1.8. Miscellaneous Provisions for Internet Use, E-mail and Other ICT Resources

3.1.8.1 Unacceptable Personal Use

Described herein are general acts considered to be unacceptable use of ICT resources. These may be acts to interrupt official business operation, cause undue loss, damage or cost to the Government, and embarrassment.

- Violation of Law. Act to violate, encourage violating, accomplice to a violation of the Government's rules and regulations and any local or national law.
- Illegal Copying. Any act of copying or any act of similar nature using copyrighted materials of any format as prohibited by copyright or intellectual property regulations.
- Operating a Business. Directly or indirectly using the Government's facility to operate any non-Government related business is prohibited.
- Gaming, Gambling or Wagering. Accessing, operating or simply viewing any gambling activity over any Government-owned ICT facility is prohibited. This

extends to computer gaming and any form of entertainment not related to official business function.

- Solicitation. Except for Government-approved programs, soliciting for money or support on behalf of charities, religious entities or political causes is strictly prohibited.
- Political or Partisan Activities. The use of any ICT facility to promote, advocate, distribute any material, or any act of similar nature, for political or partisan politics is prohibited.
- Compromise Integrity of the ICT Facility. Any act that will reduce the reliability, compromise fidelity, or any action of similar nature that will negatively affect the integrity of the ICT facility is prohibited.
- Acts that Waste ICT Resources. Any act that depletes, expends or any action of similar nature that wastes resources including but not limited to, excessive printing of documents, storing unnecessary files on hard disk drives, storing unimportant e-mails on Government provided e-mail systems, transmission/ extraction of large files over the network or internet, etc. is prohibited.
- Web 2.0 Use. Web 2.0 technologies include on-line communities, on-line forums, chat rooms, instant messaging, blogs, wikis, webo's, peer-to-peer file sharing, and social networks. Employees must obtain permission from their department supervisor and Organisation responsible for ICT implementation in Malawi to use any of these technologies in the workplace. Any employee permitted to participate in any of the above means of communication should comply with the rules and regulations of the Government, the Government's ICT policy and any related local and national law.
- Obstruction to ICT Resources. Impede, directly or indirectly cause a delay, encrypt or conceal, or do any similar act that will limit or prohibit the Government from accessing, operating, monitoring, and reviewing ICT resources is prohibited. Only authorized Organisation responsible for ICT implementation in Malawi staff shall be allowed to set or manipulate passwords on any Government-owned common ICT resources, and/or limit the use of ICT resources by specific employees with the approval of Senior Management.
- Falsification or Misrepresentation. Falsifying any electronic document or misrepresenting one's identity or association to carry out an unauthorized, unlawful, offensive act through electronic communication whether using Government-owned ICT resources or personal devices within the premises of the Government is strongly prohibited.
- Restrictions on the Use of Government provided E-mail Addresses. Government employees shall avoid use of Government provided e-mail addresses such as firstname.surname@agencyname.gov.mw for personal

communications in civil forums or sites of similar nature unless approved by Senior Management, for official purposes only. This is to avoid any personal opinion being interpreted as a Government opinion.

- Violations of Civil or Private Systems Security Measures. Any use of Government provided ICT resources to manipulate or compromise the security or operation of any Civil or private computer systems is prohibited.
- Violating Data Privacy or Confidentiality Procedures. Using Government provided ICT resources or personal device inside or outside the Government premises to violate or attempt to circumvent data or confidentiality procedures is prohibited.
- Accessing or Disseminating Private or Confidential Information. Accessing or disseminating private or confidential information about another person whether the person is an employee or non-employee of the Government, using Government-owned ICT resources without proper authorization is prohibited. Prohibition includes falsifying of such information.
- Accessing Systems without Authorization. Accessing files, systems, networks, account of another person and similar devices within the Government provided ICT resources are prohibited. Each employee is accountable for the safeguarding of their PIN, passwords or keys in accordance to related policies.
- Distributing Malicious Code. Distributing malicious code or similar format such as computer virus, spyware, malware is prohibited. Prohibition includes intentional keeping of malicious codes.

3.1.8.2 No Anticipation of Privacy

In general, no employee should expect or demand privacy in using Government provided ICT resources. At any time, with the approval of Senior Management, and for official purpose, organisation responsible for ICT implementation in Malawi may subject the ICT resource to review, inspection and investigation.

3.1.8.3 User Agreement to the Terms and Conditions of this standard:

Relative to the use of the Government ICT Equipment, Government Network Facility, Government e-mail systems, or any of the Government related ICT components and parts, the user shall agree to the terms and conditions of this standard. All Civil Service employees will be required to sign an ***Acknowledgement of Receipt and Understanding Form***, attached as Annex 8 to this standard, to certify their willingness to comply with the acceptable use provisions.

3.1.9. Disciplinary Action

The violation of the provisions of this standard will lead to disciplinary action. Penalties provided will be based on the Disciplinary Procedures set out in the Staff Manual of The Malawi Public Service Regulations (MPSR) and other pertinent civil service laws.

3.2. Electronic records management

3.2.1. Definitions

The *ICT Glossary and Definitions* contains a description of any common ICT terminology referred to in the policy and standard documentation.

For the purposes of this *ICT Standard and Guide for Electronic Records and Document Management* and all associated and related documentation and processes, the terms 'document' and 'documentation' include any recorded information or material, in electronic format, which conveys coherent information for human understanding and use.
The terms 'document' and 'documentation' also include any recorded information, including, but not limited to, textual data, graphical, visual, audio and electronic information.

3.2.2. Standard and Regulations

The *ICT Standard and Guide for Electronic Records and Document Management* applies specifically to appropriately authorized and approved documentation that is stored electronically, transmitted on the GWAN, or hosted on GoM Websites.

These document hierarchies provide repositories for electronic documentation of interest to the GoM and individual teams within Ministries/Departments. The level of accessibility granted to a specific document will be determined prior to the approval and release of that document.

ICT staff will have access to other network file storage and a range of local file storage. This document does not apply to these areas.

3.2.2.1 Regulations

- Policies and documents for inclusion in the GOM Calendar shall be reviewed by the Chief Technology Officer. Once reviewed, these documents maybe tabled and approved by various governance committees of which ICT staff are members. Once approved, they will be sent to the person responsible for amendments to the GOM Calendar for inclusion in the next update.
- All other ICT documents stored in the GOM Website, shall be approved by an appropriate ICT staff member or committee, commensurate with the level of risk, confidentiality, audience and significance of the document and issues discussed in the document.
- All documents shall be published in PDF format to preserve their integrity. The original source documents will be stored in a secure format.
- All documents that improve the level of assurance, business continuity, and delivery of the range of products and services provided by ICT shall be stored electronically.

- Each document shall contain a Document Information and Version Control statement on the first page of the document.
- All printed documents shall be treated as Uncontrolled. The Controlled version shall be the electronic version.

3.2.2.2 Objective–ICT Document Management Process

All documentation subject to this standard should adhere to the ICT Document Management Process.

The ICT Document Management Process regulates and guides the lifecycle of every document created by, and for, the Government of Malawi. In brief, the process helps ensure that each document is:

- Created in a standard and reliable format, with accurate content and common naming conventions.
- Correctly maintained to ensure continued accuracy and validity.
- Accessible from designated locations (electronic).
- Securely archived (and eventually destroyed) when the document no longer services an existing process.

3.2.2.3 Process Overview- ICT Document Management Process

The Document Management Process regulates the entire lifecycle of every document created within that process, and is comprised of the following six sub-processes:

1. Creation
2. Approval
3. Publication
4. Maintenance
5. Archive
6. Destruction

An original source copy of every published document shall be stored in the Documentation Framework site, which is a sub-site of organisation responsible for ICT implementation in Malawi Website.

This site will be used as the primary storage and workspace/collaboration area for all ICT policies, standards and guidelines. Documents shall be created, edited and maintained in this site. Once a document is ready for release, a copy shall be converted to Adobe Acrobat (PDF) format and published to the relevant location.

All URL references within a document shall be linked to the published version of the reference. An edited document when released for publication shall overwrite the existing published version, to ensure that links to the document remain valid.

3.2.2.4 Documentation Register

For each document stored electronically, the following details shall be provided:

- Location where published
- Document Title
- Date Published
- Who Published
- Review Date.

Documents will be reviewed at least annually.

3.2.3. Document Management Guidelines

These guidelines outline the various management stages of a document lifecycle from creation, approval, publication, maintenance, archive, and ultimately destruction of a document in line with the Document Management Process of the Government of Malawi.

3.2.3.1 Publishing Process Overview

The publishing process shall ensure that approved documents contain accurate and up-to-date creation, approval, and maintenance information, and that only the most recent version of any document is available for access and use.

3.2.3.2 Maintenance Process Overview

All documents shall be allocated a review period of not more than one year. In addition, all staff are required to notify an Owner where an inaccuracy or problem is identified in an approved document, and Owners must then initiate an update of the document.

The document's Review Date is typically set at 12 months from the date the document was last reviewed. Where it is believed that a document will require review within the 12 month period, a shorter period (i.e. closer Review Date) may be set, at the Owner's discretion. In any case, documents may not be allocated a Review Date exceeding 12 months from the date the document was last reviewed.

3.2.3.3 Archive Process Overview

The majority of documents stored in the Documentation Framework Site relate to the provisioning of current services, systems, and processes. In many instances,

the implementation of new versions negates the need to retain superseded version documentation.

CD and DVD copies shall be retained for a period of 7 years and then will be removed from the archive and destroyed.

3.2.3.4 Destruction Process Overview

If a document does not require archiving, it shall be destroyed either when a new version is created or updated, or when the Owner advises that the document is no longer required. Archival copies of documents will be destroyed after a period of 7 years has elapsed from the creation of the CD or DVD archive version.

3.2.3.5 Roles of various officers in Document Management

3.2.3.5.1 Senior Manager

The Senior Manager in this case is the manager of each section responsible for the process. In such cases where the Senior Manager is not available, the next person in charge can perform the tasks as required.

Note: Where a Senior Manager is also the Author and Owner of a document, another staff member must perform the Senior Manager's reviewing responsibilities.

Senior Managers shall:-

- Approve release of the document for publication after the owner has released the document for use.
- Ensure the document does not duplicate the content or purpose of an existing document.
- Ensure the document uses the correct template and file naming conventions.
- If the Owner of a document has left the section, Senior Managers must allocate any of the Owner's documents to a new Owner. In such cases, until a new Owner is allocated, the Senior Manager becomes temporary Owner of those documents.

3.2.3.5.2 Chief Technology Officer

The Chief Technology Officer is the Assistant Director (MISTMS) in organisation responsible for ICT implementation in Malawi. In such cases where the Chief Technology Officer is not available, a Senior Manager, or other delegated representative of the Chief Technology Officer, can perform the task as required.

Note: Where the Chief Technology Officer is also the Author and Owner of a document, another staff member must perform the Chief Technology Officer's reviewing responsibilities.

The Chief Technology Officer shall:-

- Schedules periodic audits of the content and quality of the Document Management Process.
- Approves modifications to the ICT Document Management Process.
- When new or amended policies, standards, or guidelines are introduced, the Chief Technology Officer assesses the implications of these new policies, standards, or guidelines, and initiates the creation of new policies, standards, and guidelines, or the amendment of existing policies, standards, and guidelines, as necessary.
- If a Senior Manager, being the Owner of a document, has left the section, the Chief Technology Officer must allocate any of the Senior Manager's documents to a new Owner. In such cases, until a new Owner is allocated, the Chief Technology Officer becomes temporary Owner of those documents.

3.2.3.5.3 ICT Staff

GOM staff is not only the end users of documentation, they also play an integral part in ensuring that document management works.

ICT staff shall ensure that:-

- They do not store obsolete documentation.
- They do not make unauthorised copies of documentation, including printed copies, electronic copies, or storage of electronic copies in unauthorised locations.
- Any undocumented process is brought to the attention of their Senior Manager, and that a document creation is initiated.
- Any modifications to a process affecting its documentation are brought to the attention of the document Owner to ensure modifications occur within one week.
- Any unauthorized documentation used by ICT staff is re-created and processed through the Document Management Process.

3.2.4. Document Management Standards

These standards outline the various syntax and regulations that will apply to the conventions applied as part of a document, in-line with Document Management Process within the Government of Malawi.

3.2.4.1 Document Title

With the exception of forms, templates, and spreadsheets, the document title appears:

- In the body of the document's cover page
- In the header of the document's cover page
- In the header of the document's body content

As part of the document's electronic file name the following exceptions apply:-

Forms:

The document title appears as part of the document's electronic filename, which is located in either the header or the footer of the document, as appropriate.

Spreadsheets:

The document title appears as part of the document's electronic filename, and is displayed in the title bar of the spreadsheet application.

Templates:

The document title appears as part of the document's electronic filename. The document title does not otherwise appear in the document.

3.2.4.2 Rules

- Document titles must accurately and concisely represent the document's purpose.
- Where a document will have the same name and/or purpose for more than one agency, the document title must include the name/acronym/initials of that section: (e.g. MOF Work Request, Organisation responsible for ICT implementation or regulation in Malawi Work Request).

3.2.4.3 Version Numbering

Version numbers shall be allocated by the Owner. Every document will have an identifying version number. With the exception of forms, templates, and spreadsheets, the version number must be displayed:

- In the Document Information table located on the document's first page

3.2.4.3.1 Version Number Formatting

Version numbering is broken down into two types:

1. Draft version numbering
2. Active Change version numbering

Draft version numbering is displayed in the following format: **V*n.n***

Where:**V**: is always presented in uppercase

n: is a number from 0 to 9.

Active Change version numbering is displayed in the following format: **V*n.n***

Where: **V**: is always presented in uppercase

n: is a number from 0 to 9.

3.2.4.3.2 Draft Version Numbering

A document is considered to be in Draft stage from the time it is created until it is approved. During creation, the document shall undergo continual review and modification until it is approved.

Draft version numbers shall appear to the right of the decimal point in the version number (the zero on the left side of the decimal point never changes in a Draft document version number). The Draft version number increases by one minor version with each review and modification. For example:

Modification	Version Number (increases)
First draft	V0.1
Second draft	V0.2
Third draft	V0.3

Where a document has gone through more than 9 drafts (i.e.V0.9), the version number format may be extended to V0.*nn* (e.g. V0.11).

3.2.4.3.3 Active Change Version Numbering

Active Changes only occur to approved documents. An Active Change is any change made after a document has been approved.

When a Draft document is approved, its version number shall change to V1.0. This is the first 'live' version of the document, and means it is approved for use. Any further changes to the document cause the version number to increase by one minor version from V*n*.1 to V*n*.9, and then increase by version in sequential order. For example:

Modification	Version Number (increases)
First change	V1.1 (was V1.0- increases by.1)
Second change	V1.2
Third change	V1.3
…	

Tenth change	V1.10
Eleventh change	V1.11
Twelfth change	V1.12

After a document has been reviewed, the version number shall change by 1 increment (e.g. review done after twelfth change, V1.12 changes to V2.0).

3.2.4.4 Related Documents Information

For Policies, Standards, Guidelines, Minutes and other documents as required, the Related Documents section of each document includes a list of documents related to the contents of that document. If these documents are stored electronically, a link should also be part of the document name.

3.2.4.4.1 Related Documents Categories

Related documents are divided into four categories:

1. Policies, standards and guides
2. Procedures
3. Forms and templates
4. Other

For each document listed in the Related Documents section, the following information is required:

- Document (Electronic): The Document file name: (e.g. Document Standards and Conventions).
- Note that neither the version number (e.g.V1.0) nor the file extension (e.g. .doc) should be included.
- Location (URL) of the published version of the document.

3.3. Information Asset Classification and Control

3.3.1. Definitions

"Information Assurance" is concerned with the protection of information and information systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation of information operations.

It includes providing for restoration of information systems by the incorporation of appropriate protection, detection and reaction capabilities.

This Information Asset Classification and Control Standard requires agencies to implement policies and procedures for the classification and protective control of information assets (in electronic and paper-based formats) which are commensurate with their value, importance and sensitivity.

All physical information assets (including hardware and software) used to process, store or transmit information must be accounted for. In addition to asset inventories, all major information assets used in an organization's operations must be identified and an owner assigned for the maintenance of appropriate security controls.

3.3.2. Standards

1) Inventories of all major information and ICT assets should be maintained;
2) Information will be classified according to its sensitivity and importance, taking into account the organization's requirements for the sharing or restriction of information, legal and/or legislative requirements and probable impact resulting from unauthorised access or damage to the information. To achieve and maintain appropriate protection of the organisational information assets:-
    - All assets shall be clearly identified and an inventory of all important assets drawn up and maintained;
    - The organization will adopt the Business Classification Scheme for the purposes of classification of "public records" and disposal schedules;
    - All information and assets associated with information processing facilities shall be "owned" by a designated part of the organisation. The owner shall be an organization's Senior Manager/System Sponsor or organisation responsible for ICT implementation in Malawi and
    - Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

3) The organization's information classification scheme will be based on the following qualifications:-
   - Information will be classified as either Public or Non-Public;
   - Non-Public Information will be classified as either Unclassified or Classified;
   - Classified Information will be classified as either Secure or Sensitive.
4) Confidentiality, integrity and availability of sensitive or secure information will be appropriately protected throughout the information lifecycle: collection; storage; use; transmission; disposal.
5) If information is stored in the Data Centre, the security classification will be commensurate with the zone where the information is located.
6) The organization's Senior Manager/System Sponsor or organisation responsible for ICT implementation in Malawi ICT Manager ("Officer") is responsible for ensuring an information technology resource and/or the information contained within, is classified as: Public; Sensitive;

7) or Secure Information. Security measures will be implemented according to the information classification.
8) Sensitive or secure information will be appropriately protected independent of location and technology. To ensure that information receives an appropriate level of protection:-
    - Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
    - An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification system adopted by the organization.
9) Authority to lower an information classification must be obtained from the owner of the information source.
10) Organization employee or citizen personal information shall be classified as at least sensitive information.
11) Core Information Systems will be identified and information assurance responsibility assigned to the Core System Sponsor unless otherwise indicated.
12) Organization Staff should agree to a confidentiality agreement prior to commencement of formal duties and the agreement should be reviewed annually or whenever there is a change in terms of employment.
13) Classification schemes do not limit the provision of relevant legislative requirements under which the organization operates.
14) Disposal of public records shall be in accordance with the organization's Records Disposal Policy.
15) The archiving of information and documents shall be in accordance with the organization's Archives Policy and Procedures.
16) Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.
17) Removal off site of the organization's sensitive information assets, either printed or held on computer storage media, should be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out. At a minimum, where information is classified as "Classified – Secure" or "Classified – Sensitive", a Confidentiality Agreement between the organization and the Organisation contracted to perform services for the organization where access to this information is required shall be signed and processed through the appropriate Legal Office.
18) Responsibility remains with the organization, therefore these obligations must be considered when entering into arrangements that permit access to sensitive and/or secure information with a third-party (e.g. vendor support, contractors, associated organisations).

19) Procedures to ensure the confidentiality, integrity and availability of information should be considered in conjunction with, but not limited to the following recommendations in respect to the information lifecycle:-

Collection	• The source of information should be considered prior to making decisions (labelling, etc.) based upon its confidentiality or integrity: • Low: received from an unreliable source and has not yet been confirmed • Medium: received from associated organisation, validated and confirmed • High: received from a reliable source that has been confirmed • Collection of information is covered by the Organization's Privacy Standard/Statement and can only be used for its intended purpose. • Aggregated data may result in an information classification higher than the individual data. E.g. User-ID (public), Password (Public), User-ID/Password (Secure) • Data volume may also require information classified at a higher level than individual data. e.g. 1 User-ID/Password (Sensitive), Multiple User-ID/Password (Secure)
Storage	• Clear Desk Standard: The Government advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons. Secure in lockable container, or at least lock office when unattended. • Password protected screen saver and/or always lock workstation when unattended • Computer Access Controls: password protects sensitive information, encrypt secure information.

	• Segregation of duties. • Operating procedures for handling of computer media (tapes, disks, diskettes, printouts, system logs) and system documentation.
Use	• Approval and authorisation of access by information owner • Annual confidentiality agreement procedure • Privacy Statements • Access audit
Transmission	• Post: Certified mail, signed receipt or confirmation required for secure information. • Facsimile: Require phone call to receiving party before transmission, advised when message received. • Network transmission: Consider SSL (Secure Socket Layer) for sensitive information, required for secure information. • Web-accessibility: Only necessary information should be made available.
Disposal	• Paper: sensitive information should be shredded; secure information disposed using secure disposal service and considers shredding in addition before disposal. • Computer Disk: containing sensitive information should be re-formatted at least twice, secure information consider using commercial programs or service to wipe information off the media in a more secure manner.

3.3.2.1 Information Asset Security Classification Controls

The following Information Asset Security Classification Controls are based upon those outlined in the Government of Malawi Information Security Classification.

3.3.2.1.1 Public

Refer to Schema for Unclassified (following)

3.3.2.1.2 Unclassified

	UNCLASSIFIED information is official information that is not in the public domain, but does not otherwise need to be classified. UNCLASSIFIED information is information which still needs to be protected and controlled, and is not to be considered PUBLIC information. Official information needs to be specifically classified as PUBLIC before it is released. It may be helpful to mark information with this classification level so that it is known that the assessment has been made. Information which has not been assessed is best marked Not-Yet-Security-Assessed or with some similar identification and should be treated as UNCLASSIFIED. UNCLASSIFIED information may be marked as INTERNAL-USE-ONLY, or UNCLASSIFIED.
Collection	**Preparation and Handling** *Markings* Not required, though helpful in distinguishing UNCLASSIFIED information from information that has not been classified. *Page Numbering* Optional, but generally helpful. *Filing*: File in accord with normal records management practices. *User Auditing* Log in, logout, failed attempt. *Printing* No special requirements.
Storage	**Copying and storage** *Copying* To be kept to a minimum in accord with operational requirements. *Storage* Maybe stored in unsecured cabinet. *Electronic Storage* Common access drive or directory.
Use	**Removal from workplace, and monitoring** Removal of file or document only on a basis of need. *Monitoring* None required. **Discussing Unclassified Information** *Meetings* No restriction but basis of „need-to-know“ *Telephone and video-conference* May be passed in the clear (unencrypted) over communications systems.

Transmission	**Manual Transmission** *Within a single location* May be passed uncovered by hand. Passed by internal mail in a use again envelope. *Between locations* Passed by internal mail in a use-gain envelope. Passed by external mail in an opaque envelope. **Electronic Transmission** *Data transmission* Basis of „need-to-know". May be passed by data transfer using internal or external networks including the internet. *email* Basis of „need-to-know". May be passed by e-mail using internal or external networks including the internet. *Fax* Unclassified information may be passed in the clear (unencrypted) by fax.
Disposal	**Archive & Disposal** In accordance with authorised retention and disposal schedule issued under the Organization's *Records Disposal Policy*. *Paper waste* Drafts, working papers and copies may be recycled. Drafts, working papers and copies may be discarded with general paper waste. *Electronic Media & equipment* Media may be reused or disposed of as per paper waste.

3.3.2.1.3 Classified- Secure

	Information whose compromise could cause damage to the Government, commercial entities or members of the public. For instance, compromise could: • endanger individuals and private entities; • work substantially against Organization's finances or economic and commercial interests; • substantially undermine the financial viability of major organisations; or • seriously impede the development or operation of major Government policies. As a principle, most non-national security information would be adequately protected by the procedures given to information marked X-IN-CONFIDENCE or PROTECTED.

Collection	**Preparation and Handling** *Markings* Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20point) bold and red if possible. *Page Numbering* Desirable. *Filing* File in distinctive file (green). Appropriate file cover sheet to be used. *Preparation of Electronic Information* Prepare in drive or electronic document and records management system with restricted access. *User Auditing* Log in/out, failed attempt, Read, Write and Delete. *Printing* Printer not to be left unattended while PROTECTED documents are being printed.
Storage	**Copying and storage** *Copying* May be prohibited by information owner. To be kept to a minimum in accordance with operational requirements. *Physical Storage* „Clear Desk" policy. Key lockable steel container (C-Class) in a secure or partially secure environment. Steel-lined, tamper-evident container with a combination lock (B-Class) in an intruder resistant environment. *Electronic Information Storage* Restrict logical access based on need-to-know.
Use	**Removal from workplace, and monitoring** *Removal of file or document* Basis of need. Authorisation of information owner required. Kept in personal custody. Ensure adequate storage arrangements. *Monitoring* Regular checks of the Security Classified Information Register and information are desirable. **Discussing Classified Information** *Meetings* Must occur behind closed doors in fully enclosed rooms. Notify classification to audience. Material must include classification markings. Remove from equipment and white boards prior to vacating room

	Telephone and video conference Telephone and video conference should not be used for data or voice transmission of material unless both ends are provided with encryption. Cordless or mobile phones should not be used to discuss protected information unless the security they use has been approved for this classification.
Transmission	**Manual Transmission** *Within a single location* Single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff indiscrete office environment. Should not be left unattended on recipient's desk. *Between locations* Double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); or Single opaque envelope that does indicate classification and secured in a lockable container and delivered by an authorised messenger. Receipting required. **Electronic Transmission** *Data transmission* Basis of "need-to-know". May be passed over appropriately classified internal networks. Information should be encrypted when being sent between agencies using Transport Layer Security (TLS), Secure Sockets Layer (SSL) or IP Security (IPSec) encryption. *e-Mail* Basis of "need-to-know". May be passed over appropriately classified internal networks. Information must be encrypted (e.g. via secure e-mail) when sent between agencies. *Fax* Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encrypted communications systems must be used to transmit PROTECTED information.
Disposal	**Archive & Disposal** In accordance with authorised retention and disposal schedule issued under the *GOM/Organization's Records Disposal Policy*. *Paper waste* Drafts, working papers and copies must be shredded. *Electronic Media & equipment* Media to be destroyed or sanitised.

3.3.2.1.4 Classified- Sensitive

Information whose compromise could cause limited damage to the Government, commercial entities or members of the public, including:

- cause distress to individuals or private entities;
- cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or private entities;
- prejudice the investigation or facilitate the commission of crime;
- breach undertakings to maintain the confidentiality of information provided by third parties;
- impede the effective development or operation of Government policies;
- breach statutory restrictions on the management and disclosure of information;
- disadvantage the Government in commercial or policy negotiations with others; or
- undermine the proper management of the Government and its operations.

This protective marking is accompanied by a notification of the subject matter which alludes to its audience and the need-to-know principle. Examples include:

STAFF-IN-CONFIDENCE
Includes all official staff records where access would be restricted to HR personnel and nominated authorised staff. For example, personal files, recruitment information, grievance or disciplinary records.

EXECUTIVE-IN-CONFIDENCE
Information associated with executive management of the entity that would normally be restricted to the executive and nominated authorised staff. For example, sensitive financial reports, Strategic plan, Government matters, Staff matters, etc.

COMMERCIAL-IN-CONFIDENCE
Procurement/contract or other commercial information such as sensitive intellectual property. For example, draft request for offer information, tender responses, tender evaluation records, designs and government owned research.

AUDIT-IN-CONFIDENCE
Information related to audit activities where access would be restricted to officers of the Audit department or nominated authorised staff. For example, Audit and Risk reports which identify security and control weaknesses.

Collection	**Preparation and Handling** *Markings* Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20point) bold and red if possible. *Page Numbering* Desirable. *Filing*: File in distinctive file (blue). Appropriate file cover sheet to be used. *Preparation of Electronic Information* Prepare in drive or electronic document and records management system with restricted access. *SCI Register* Desirable. *User Auditing* Log in/out, failed attempt and Delete. *Printing* Unless otherwise secured, Printer not to be left unattended.
Storage	**Copying and storage** *Copying* May be prohibited by information owner. To be kept to a minimum in accordance with operational requirements. *Physical Storage* "Clear Desk" policy. Lockable cabinet. *Electronic Information Storage* Restrict logical access based on need-to-know.
Use	**Removal from workplace, and monitoring** *Removal of file or document* Basis of need. Authorisation of information owner required. Kept in personal custody. Ensure adequate storage arrangements. *Monitoring* Basic checks only, no need for formal audit. **Discussing Classified Information** *Meetings* If discussions are held, care should be taken to ensure that people without a need to know are notable to overhear the discussions. If a meeting is held, Remove from equipment and whiteboards prior to vacating room. *Telephone and video conference* May be passed in the clear (unencrypted) over internal

	communications systems. Between sites, encryption is desirable but not mandatory.
Transmission	**Manual Transmission** *Within a single location* Single opaque envelope indicating classification. Uncovered by hand indiscrete office environment. *Between locations* Single opaque envelope that does not indicate classification. Receipting at discretion of information owner. Delivered by hand or authorised messenger. **Electronic Transmission** *Data transmission* Basis of „need-to-know". May be passed unencrypted over appropriately classified internal networks. Information should be encrypted when being sent between agencies. *Email* Basis of „need-to-know". May be passed unencrypted over appropriately classified internal networks. Information should be encrypted (e.g. via secure e-mail) when sent between agencies. *Fax* Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encryption is desirable but not mandatory
Disposal	**Archive & Disposal** In accordance with authorised retention and disposal schedule issued under the *GOM/Organization Records Disposal Policy*. *Paper waste* Drafts, working papers and copies may be recycled through lockable classified waste bins. Drafts, working papers and copies may also be shredded. *Electronic Media & equipment.* Media may be reused or disposed of as per paper waste.

3.4. Information Systems Security Management

3.4.1. Introduction

3.4.1.1 Goal

Support the Government of Malawi (GoM)/Organizations, through the organisations responsible for ICT implementation or regulation in Malawi, in running one of its core functions, namely: development and implementation of information systems and technology develop and manage integrated information technology infrastructure, optimization of resource utilization and installed infrastructure.

Protecting the confidentiality, integrity, and availability of information assets from any disruption and threats both from within the organisation or from external parties, whether intentionally or otherwise.

3.4.1.2 Scope

This standard applies to all assets used to secure the management of GoM/Organization information, and is used within all organisations and related units as well as providers and users of GoM public service. The scope is also defined in terms of organization and locations. This standard applies at organisation responsible for ICT implementation in Malawi and all units throughout GoM, relevant government agencies, business partners and other third parties.

3.4.1.3 Definition

1. Information asset in this standard is information and the processes of its gathering, processing and distribution. Information assets include:-
    a) ***Data/documents:*** Economic and financial data, payroll data, personnel data, tender documents and contracts, document management system(s).
    b) ***Software:*** Application software, system software, system development toolkit, and other assistive devices (antivirus, audit tools).
    c) ***Physical infrastructure:*** Computer equipment, networking and communications equipment, removable media (e.g. flash, CD, DVD, diskettes), and other supporting equipment (e.g. UPS, generators, communications antenna).
    d) ***Intangible assets:*** Including knowledge, experience and expertise, image and reputation.
2. Information Security Management Policy is a framework for security management of information assets using a risk based approach in formulating, implementing, executing, monitoring, reviewing, maintaining and improving information security performance.
3. Information Asset Owner is the party that is legally designated as being responsible for the information asset or work processes in the

GoM/Organization or the management of organizational units where the data or information was created or is stored.

4. Chief Information Security Officer is an official appointed by the ICT Steering Committee to coordinate and direct the activities of the application of information security policies and procedures within the agency where he/she is assigned. The Chief Information Security Officer is to coordinate with similar officials in other agencies either directly or through the Information Security team to resolve existing problems.
5. Permissions are powers/rights related to the use of an asset type and level of information tailored to the needs of a specific business process, that has been granted based on related information security risks. This right, depending on the type of asset, is formally granted or authorized by the owner of the asset.
6. Risk assessment is the entire process of analysis and risk evaluation.
7. Risk Evaluation is a process that compares the estimated magnitude of a risk with already well-defined criteria to assign levels of risk.
8. Information security incidents are events that are not desirable and that violate the policy or procedures of the ISMS that poses a threat to the security of information assets or results in disruption of the work process of the organization.
9. Mobile Computing is the use of portable computing devices (portable), such as notebooks and personal digital assistants (PDA) to access, data processing and storage.
10. Tele-working is the use of telecommunications technology to enable employees to work at a remote location from the office.

3.4.1.4 References

I. ISO / IEC 27001:2005 Information Security Management System, Standard
II. ISO / IEC 27002:2008 Information Security Management System, Guidelines
III. ISO / IEC 27005 (BS7799-3: 2006) Risk Management System

3.4.2. Information Security Management Policy

3.4.2.1 General Policy

1. Comply with all laws and regulations applicable including the legal obligations to protect its information assets.
2. Comply with the requirements as well as operational and technical standards as contained in the overall information security policies and procedures related to ISO / IEC 27001:2005 standard and is formally applicable to all organizations.
3. Identify and establish ownership-of or responsibility-for managing all information assets.

4. Carry out a review and manage information security risks associated with target activities and maintain continuity plan activities. Security risks are assessed at least once a year.
5. Conduct internal audits by an independent party at regular intervals to check compliance with policies, requirements, standards and procedures for information security, at least once a year.
6. Improve operational performance by evaluating the results of information security operations, assessing the level of compliance of information security framework and implementing any required corrective measures.
7. Working closely with Organizations and the relevant government agencies to improve the security of data and information exchange.

3.4.2.2 Leadership Responsibilities

1. Directly accountable for the consistency and effectiveness of information security management implementation within organizations.
2. Make efforts to increase awareness of information security by disseminating this information security policy for all leaders and employees of the organizations, related government agencies, business partners and other third parties who do the work / provide services to the GoM/Organization.
3. Improving the knowledge and skills of information security personnel through education, training, and socialization as needed.
4. Establish annual targets to be achieved by the process of managing information security, which is realized through the supervision and direction of the whole process of preparation and implementation of an information security work program on an on-going basis, which is intended to maintain and enhance long-term effectiveness, by providing appropriate resources.
5. Ensure availability of all resources (human, facilities, and budget) needed to implement information security policies.

3.4.2.3 Documentation Information Security Management

1. GoM/Organization is committed to develop and maintain documentation of information security management that consists of policies, procedures, standards and records.
2. Documentation of information security management should be made available in all areas of operations and accessible to users who require them. They shall be updated, maintained and protected from unauthorized use.

3.4.3. Third Party Security

3.4.3.1 Third Party Access Security

Access to information assets within GoM/Organization must be strictly controlled. Before providing access to partners, service users, departments / other agencies

involved or other third party, the associated risks in connection with the provision of access must be identified and evaluated such that adequate controls may be implemented to reduce the impact or prevent the occurrence of those risks.

The evaluation must cover the following aspects:-

1) Type of access required:
2) Physical access to the office, workspace or server room(s).
3) Non-physical access into the network, database and information system.
4) Reason and needs access:
5) To provide support to hardware and/or software.
6) Audit of information security.
7) Development of applications and information systems.
8) Access methods, such as access via local network or access via modem (dial in) or IP VPN facilities.
9) Controlling the risks related to granting access to a third party must be specified in clearly-defined clauses and Non-Disclosure Agreement/NDA.
10) Contractual agreements with third parties must include, among others:
11) Third party liabilities are in compliant with information security policies enforced within the GoM.
12) Tacit agreement to comply with all policies related to the protection of information assets once access has been granted.
13) Type of access provided and procedure to use such access.
14) The identity of third-party employees who use this access.
15) Restricted locations where access can be done and time/period when the access may be used.
16) Confirmation of the right of GoM to monitor and control use of access.

3.4.3.2 Use of Third Party (outsourcing/sub-contract) by GoM Partners

Partners who employ third parties to provide services to the GoM/Organizations or in carrying out either part or all of their work, shall ensure that all applicable GoM/Organization information security requirements are written in the contract agreement between the partners concerned and the service providers.

Contracts referred to in the clause above shall include:-

1) Assurance that all parties involved in the contract concerned are aware of their responsibilities to the security of GoM/Organizations information assets.
2) Security controls, both physical and non-physical, must be applied to restrict access to GSO information, and only to authorised employees / users.
3) Legal responsibility (legal aspects) of any information security breach during the delivery of services or in carrying out the work as stipulated in the contract.

4) The identity of resources involved in the contracted activities.
5) GoM/Organizations shall ensure the availability of all resources (human, facilities, and budget) needed to implement information security policies.

3.4.4. Asset Classification and Control

1) All information assets and other assets associated with the security management of information are to be identified, recorded, valued and ascribed an owner. These assets include:-
    - Information assets - databases and data files, system documentation, user manuals, training material, operational or support procedures;
    - Software assets - application software, development tools and utilities;
    - Physical assets - computer equipment, communications equipment, magnetic media, site security;
    - Services - computing and communications services.

2) Each category of assets is to be recorded in an inventory. These inventories may be created in conjunction with other GoM/Organization business needs, e.g. business services, and/or as part of an overall GoM/Organization asset management system.

3) GoM/Organization information assets will have a protective marking (e.g. classification label), that reflect requirements for their Confidentiality, Integrity and Availability. These protective markings are to be ascribed in accordance with current GoM/Organization guidance.

3.4.5. Personnel Security

1) Security is to be an element of GoM's/Organization's human resources management processes. Personnel security measures are required to reduce the risks to information systems arising from human error, theft, fraud or misuse of information assets.

2) GoM/Organization Senior Management, staff and staff of third party suppliers will undertake security vetting according to the value of the sensitive information they have access to in the course of their work. They will be required to sign a confidentiality/non-disclosure agreement with GoM/Organization.

3) The GoM/Organization HR & Service departments will provide staff with security training as part of the induction process and as part of the user training for information systems. Input to security training material will be provided by other departments as needed. Security awareness will be programmed as a regular official activity. Third party suppliers will be

required to demonstrate that their personnel security measures are consistent with the GoM/Organization security policy.

4) All GoM/Organization officials and members of GoM/Organization staff are to report all security related incidents to their line managers or though other specified channels as appropriate. Reporting is required of all security incidents, software malfunctions and suspected security weaknesses in systems or procedures.

5) GoM/Organization human resource management processes are to include procedures for handling employees who may have violated this information security policy or any of the security procedures, security manuals or other security related guidance documents.

3.4.6. Physical and Environmental Security

1) GoM/Organization physical security measures are to address risks to all GoM/Organization assets, including information assets.

2) There is to be particular focus on preventing unauthorised physical access to Office premises especially in any shared accommodation.

3) Physical and environmental measures to protect equipment are to take account of the risks of accident, everyday hazards of theft, fire, flood and power failures.

4) Remote workers shall ensure that the GoM/Organization information assets in their environment are adequately secured against misuse, loss, theft, and/or damage. They must use properly secured equipment for sensitive work. Guidance on this will be provided in security procedures.

5) Physical and environmental measures of third party suppliers are to meet GoM/Organization requirements and standards.

3.4.7. Communications and Operations Management

1) GoM/Organization requires comprehensive management of its communications and operations systems. Operating procedures for the GoM/Organization information systems are to be documented and maintained. Change control processes are core to the proper management of information systems and these are to be fully documented.

2) Responsibilities for the proper operation of the GoM/Organization information systems are to be documented; duties are to be segregated as much as possible to reduce the risk of negligent or deliberate system misuse.

3) Software and procedural controls are to be in place throughout GoM/Organization information systems to minimise the risk of intrusion of a virus or malicious software.

4) The connections to GoM/Organization electronic information systems from systems owned by other organisations are to be protected in collaboration with the other organisations.

3.4.8. Controlling Access to Information

1) GoM/Organization business needs define the access requirements for GoM/Organization Senior Management and staff to information systems. GoM/Organization information system users will be grouped into user groups for the purpose of managing access to GoM/Organization information systems. The need-to-know principle will underpin all GoM/Organization access management procedures.

2) User accounts are to be created for users of GoM/Organization information systems. These are to be reviewed regularly by administrators to ensure that authorisation processes remain sound, including effective passwords; in particular administrators are to check that all user accounts are actively required.

3) Access to all GoM/Organization networked or standalone computer services, and intelligent network devices, is to be via a secure log-on process designed to minimise the opportunity for unauthorised access. Each user of a computer system must be uniquely identified to the system. Where passwords are used, they will be managed in a secure manner to ensure their confidentiality and integrity. The process of authentication of a user to a system will include allocation of access rights to the data and facilities needed by the user's business role.

4) Users' access to data will be controlled and monitored in order to demonstrate conformance with the requirements of the information security policy.

5) Access control measures for users' remote electronic access and contractor remote diagnostics are to be robust in accordance with the security requirements of the GWAN/Organization security policy.

6) Access control measures for system administrators are to be particularly robust to reflect the privileged access they will have to GoM/Organization information systems. Particularly strong physical, environmental and personnel security measures are to be used in support of access control measures for system administrators.

7) Electronic GoM/Organization systems security measures are to include timed lockout processes for inactive terminals.

8) Users' activities on GoM/Organization information systems will be audited in accordance with current GoM/Organization guidance in order to ensure conformance with the security policy.

3.4.9. Procurement, development, and maintenance of information Systems

1) GoM/Organization systems will be developed in such a way that security is a fundamental element of the development project in accordance with GoM/Organization information security policy and procedures. Development of an appropriate and agreed security regime will be integral to any proposal from a third party supplier for a GoM/Organization information system.

2) GoM/Organization shall clearly define and document security requirements of relevant information prior to construction, expansion, or procurement of a new information system.

3) The security of all GoM/Organization systems being developed will be subject to an accreditation process and a third party security health check to ensure that appropriate security measures are provided.

4) Information concerning the development of the information system for GoM/Organization will be confined to GoM/Organization staff and third party suppliers. Information concerning the development of system security measures will be confined to GoM/Organization and third party suppliers' staff that have a need to know.

5) All aspects of any required cryptographic and encryption key management will be undertaken in accordance with GoM/Organization standards and procedures.

6) Each software package developed by third parties (partners or other third party) used in GoM's/Organization's information systems must be free from deactivation mechanisms that can be triggered by external partners or other third party without the knowledge of GoM/Organization.

7) Technical vulnerabilities in GoM/Organization information systems must be identified, their risks assessed and controls established to prevent their exploitation or effectively resolve the weaknesses.

3.4.10. Information Security Incident Management

1) Disturbance/security incidents are evaluated periodically to ensure effective management, examine preventive measures that have been done, and plan how early detection of the incident.

2) Security weaknesses could result in imposition of disciplinary measures/sanctions to the staff responsible for the weaknesses.

3) Every computer user, whether employees, partners or third party personally responsible for ensuring that his actions did not cause or potentially cause security vulnerability information.

4) GoM/Organization must provide working tools to follow up and resolve any reported information security incidents quickly and effectively.

5) Information Security team should evaluate the report and completion of information security incidents to identify the type, volume and costs related to monitoring and performance evaluation purposes.

6) All data and records necessary to analyse and resolve information security incidents shall be secured. Records of incidents associated with civil or criminal actions, shall be secured/protected in line with applicable laws and regulations.

3.4.11. Business Continuity Management

1) Business Continuity Management will ensure that the highest priority GoM Public Services/Organization and other high priority official activities are able to continue whatever damage impacts GoM/Organization information assets.

2) A framework of business continuity plans will be produced for GoM/Organization. These plans will be regularly tested and kept under periodic review commensurate with prevailing threats to GoM/Organization assets and changes in the GoM/Organization business environment.

3) Appropriate system and data backups will be undertaken, securely stored, and periodically tested, to ensure minimum disruption to business processing in the event of an incident requiring systems and or data to be restored to a position prior to the incident. Data back-ups will be taken at least once every 24 hours of normal working operation and stored securely off site.

4) GoM/Organization has developed an ICT Service Continuity Management Policy for the whole process of service-related activities vital to reduce the impact of ICT-based information systems failures or disasters that can affect the activities of GoM/Organization.

5) To ensure that Business Continuity Management remain relevant and effective, all recovery plans shall be tested regularly, at a minimum once a year. The results of these tests shall be analysed and any faults in the plans shall be corrected.

3.4.12. Compliance

1) All GoM/Organization users are required to comply with all relevant legal statutes, licensing agreements, and GoM/Organization Policies.
2) GoM/Organization ensures that any provisions of law and legislation relevant to information systems owned by the GoM/Organization will be identified, documented and maintained.
3) GoM/Organization retains the right to access and review any document or file stored on GoM/Organization equipment and shall do so to ensure that no policy, agreement, or legal statute is contravened. Such review will be performed with the authority and knowledge of relevant officials under guidelines produced for monitoring conformance with the GoM/Organization data access policy.
4) Only authorised users shall have legitimate access to e-mail and Internet facilities provided by GoM/Organization. Limited personal use shall be permitted but all use must be in accordance with the Acceptable Use provisions of the GoM Public Service/Organization ICT Strategy and is not to include distasteful, derogatory or obscene material. Unauthorised access to pornographic or other sites containing offensive material or other serious misuse will result in GoM/Organization instituting disciplinary proceedings.
5) There will be a usage policy as part of GoM/Organization human resource management processes. This standard will address GoM/Organization users' use of e-mail and Internet both to reduce security risks and to ensure that users conform to GoM/Organization acceptable use policies of proper use of GoM/Organization information systems. This standard will also inform users that GoM/Organization will routinely monitor system usage to ensure user compliance with this standard.
6) All software installed on GoM/Organization computer system shall be properly licensed. Unauthorised copying of GoM/Organization-owned software is not permitted and is a violation of GoM/Organization copyright policy and provisions. Periodic inspection of installed software licenses will be made to ensure this standard is implemented effectively.
7) All creative ideas and discoveries by GoM/Organization employee during his/her employment, and produced by resources owned by the GoM/Organization, are to become the exclusive property of GoM/Organization.
8) Important records used or generated by information systems / information assets managed by GoM/Organization (databases, audit logs, transaction logs) should be protected from loss, damage or abuse, in line with applicable laws/regulations.

9) Third-party access to information processing facilities owned or managed by GoM/Organization may only be granted to personnel with appropriate level of competence, and complying with GoM/Organization information security policies.

10) All employees of the GoM/Organization, partners and other third parties are prohibited from using vulnerability scanning software or any software that would circumvent system security mechanism without formal authorisation from GoM/Organization Information Security Officer.

3.5. Data Back-up

3.5.1. Preamble

Organisation responsible for ICT implementation in Malawi shall manage, operate, and support a large number of computer systems throughout the Government of Malawi/Organization. In the event of any of these systems encountering data loss, each system should be covered by a data backup regimen.

The data backup regimen is a system of recording identified data onto portable media. This media is then stored both on-site and off-site to limit total loss in case of a declared disaster. The media contains a copy of specific data as at a specified time. The backup regimen is developed in conjunction with the client to meet both business and legislative requirements.

If that data is required for recovery, a data restore may be performed from the back up media.

This standard does not apply to personal devices including desktops, laptops, PDAs and USB storage devices such as USB hard drives and USB sticks. The backup and recovery of data on these devices is the responsibility of the individual user.

3.5.2. Data Backup Schedule

All computer systems operated, managed and/or supported by Organisation responsible for ICT implementation or regulation in Malawi are covered under a Service Level Agreement (SLA) between Organisation responsible for ICT implementation or regulation in Malawi and the client. The SLA contains a proviso for the client's computer system – ensuring continuity of data access and protecting the client from data loss due to systems failure, virus, vandalism, operator error, or accidental erasure.

Where a SLA covers a computer system, and a backup regimen has been requested for that system, then the system is included in the data backup schedule. Prior to including the computer system in this schedule, the client will have determined which components and data they require to be backed up as per business and legislative requirements, which could include conducting a business risk assessment, which is dependent on:-

- Importance of the data and information to the organization;
- Acceptable transaction loss (business areas must determine what level of potential transaction loss would not be acceptable or would be too difficult to recover. This can be determined in terms of a timeframe, the number of transactions, or the amount of time and effort required re-entering data);
- The maximum acceptable outage of the system while performing backups; and

- The maximum acceptable outage of system while recovering data.

3.5.3. Back-up Components

The following are the components of a back-up regimen for a computer system. Component selection is agreed between Organisation responsible for ICT implementation or regulation in Malawi and the client, and documented in a SLA, prior to the first scheduled back-up for that system being initiated.

Data to be backed up may include:

Data Type	Description
Business Data	Memos, documents, customer information, financial records, databases, accounting information, project data, schedules and appointments, e-mail, and other critical files.
Systems Data	Software and hardware configuration data, software applications, user Ids, access rights, directory structures, passwords, e-mail configurations, and any other specialised systems information.

3.5.3.1 Backup Types and Frequency

All backups occur in line with a planned Data Back-up Schedule created by Organisation responsible for ICT implementation or regulation in Malawi to meet client requirements. There are three types of back-ups used by Organisation responsible for ICT implementation or regulation in Malawi:

Back-up Type	Description
Full back-up	A complete copy of a computer system.
Incremental back-up	A copy of only the data updated since the last full or incremental backup.
Image copy	Where a computer system is virtualised, a copy of the virtual server is backed up.

Each of these back-up types may be performed at different frequencies or in combination:-

- Daily
- Weekly
- Monthly
- Quarterly

- Yearly

Typically, data back-ups are performed:-

- **Daily:** for data that changes on a daily basis.
- **Per an established schedule:** for data that changes at scheduled intervals, or to respond to major system events.
- **At month, quarter and year end:** for systems with closing dates.

3.5.3.2 Media, Equipment, and Utilities

All media, equipment and backup utilities (backup management software and in-house programs) used to perform backups are tested prior to live use. This testing determines compatibility with computer systems, storage environment, and backup frequencies.

- Where media is found to be faulty after specific testing, media is replaced.
- Vendor contact details for support and maintenance of backup hardware is on hand to ensure service contingency.
- Backup utilities are supported either by Organisation responsible for ICT implementation or regulation in Malawi or vendor staff to ensure correct operation and backup success.

3.5.3.3 Storage

Backup media is stored both on-site and off-site. On-site storage is located within a physically secure and fire-proof area of GOM/organisation.

Off-site storage is in a secure and monitored location physically distant from the source location premises. Authorised Organisation responsible for ICT implementation or regulation in Malawi employees has 24x7x365 access to this location.

All media is securely stored whether in the on-site or off-site location, or in transit. Media is not stored in any location other than those authorised by Organisation responsible for ICT implementation or regulation in Malawi.

3.5.3.4 Back-up Media Disposal

Obsolete backup media will be disposed of in a safe and secure manner in accordance with the Archived Data Retention and Disposal Schedule.

Back-up media to be disposed of must be rendered unreadable through an appropriate means. An audit-trail of disposal of back-up media will be maintained.

3.5.3.5 Backup and Recovery Documentation

Back up documentation should include the following items necessary to perform essential tasks during a recovery period:-

- Identification of all critical data, programs, documentation and support items;
- Clear documentation on how to do the backup and restore;
- Specified period of maximum acceptable outage (MAO) for all systems;
- Backup media storage locations;
- Required backup frequency, e.g. daily, weekly;
- Required backup cycles;
- Backup retention period (as per business and legislative requirements);
- Testing regimen and process;
- Recovery schedule and plan; and
- Location of relevant software and licenses.

Back-up and recovery documentation will be reviewed and updated regularly to account for new technology, business changes, and migration of application to alternative platforms.

Documentation of the restoration process will include procedures for the recovery from single- system or application failures as well as for a total data centre disaster scenario.

3.5.4. Data Restoration

All back-up data is accessible through data restoration. Data restores are performed within a physically secure area of Organisation responsible for ICT implementation or regulation in Malawi by authorised Organisation responsible for ICT implementation or regulation in Malawi employees. Restores are performed using tested utilities.

Before a restore is initiated, the client will have specified which files are to be recovered, and where those files are to be placed.

Client requests for data restores are only undertaken where the request is authorised by client management.

3.5.5. Quality Assurance and Exceptions

On the completion of a backup, success is verified using a backup log that monitors the files being backed up. Designated Organisation responsible for ICT implementation in Malawi employees check backup logs on a regular basis as part of their standard duties.

Backup successes and failures are noted in a Backup Status Log. All failures are investigated, and any problems corrected in accordance with the terms of the SLA.

By default, every backup should complete with a data capture of 100% success rate. This standard is vital to the principle of quality data access continuity in the event of the need for a data restore.

3.5.5.1 Exceptions

Although the back-up success rate should be 100%, there are allowable exceptions to the rule. A back-up may fail either partially or fully in the event of a major power failure, a major power surge, because the files are in use or hardware and software failure.

3.5.5.1.1 Major Power Failure

A major power failure may lead to systems being powered by the Uninterruptible Power Supply (UPS). However, the UPS is not designed to provide maximum and indefinite use. The source computer system containing files scheduled for back-up may have to be shut down during an outage, and/or the outage could affect the computer system driving the backup device. Both cases would make it impossible to perform a data backup at that time.

3.5.5.1.2 Major Power Surge

Although greatly reduced due to the presence of the UPS, a major power surge could damage either the source computer system or the system driving the backup device.

3.5.5.1.3 File in Use

Some computer systems require that no file is accessed or open during a backup. Where a client is using a file, rendering it unable to be backed up, and the result is the client's responsibility. This includes access by authorised representatives and unauthorised persons through the fault of the client.

3.5.5.1.4 Major Power Failure

A major backup hardware or software failure may lead to backups not being completed or performed. In this situation, if appropriate, the backups will be rescheduled.

3.5.5.2 Backup and Recovery Verification

Backup and Recovery procedures will be tested and verified on regular basis or as required.

3.5.6. Responsibilities

Both organisation responsible for ICT implementation or regulation in Malawi and the client have responsibilities in respect of data back-ups.

3.5.6.1 Organisation responsible for ICT implementation or regulation in Malawi Responsibilities

Organisation responsible for ICT implementation in Malawi should be responsible for:-

- Configuring a fully tested backup system (including media, equipment, and utilities) and data restoration capabilities;
- Securing a comprehensive vendor support and maintenance contract (including replacement);
- Ensuring all data that the client has requested to be backed up is backed up in accordance with the client's SLA;
- Initiating, managing, and monitoring all data back-ups;
- Reporting back-up successes and failures to the client on the basis and frequency agreed to in the SLA;
- Ensuring all back-up failures are investigated and examined to ensure process integrity;
- Ensuring all faults affecting backup integrity are addressed within the agreed support timeframe documented in the SLA;
- Formulating and documenting support, guidance, and operational policies, processes, and procedures in support of all back-up activities;
- Secure storage of media within GOM/Organization and at the off-site storage facility;
- Ensuring all client data is inaccessible to unauthorised persons;
- Modifying backup characteristics/requirements when formally requested by the client;
- Notifying the client as far in advance as possible of any changes affecting the client's backup (e.g. time, quality, frequency etc.); and
- Ensuring that backup media is rendered unreadable prior to disposal and media is disposed of in an appropriate manner.

3.5.6.2 Client Responsibilities

The client, and any authorised representative of the client, is responsible for:-

- Accurately identifying and documenting all data to be stored in their backups in accordance with business and legislative requirements;
- Notifying organisation responsible for ICT implementation or regulation in Malawi (via the procedure documented in the SLA) of the required backup regimen, and of any changes to that frequency. Ensuring the backup regimen meets all business and legislative archival requirements;
- Requesting organisation responsible for ICT implementation or regulation in Malawi to perform a data restore via the channels documented in the SLA; and
- Ensuring all files are free and available for backing up at the scheduled time.

3.5.6.3 Exceptions

The details in this standard may be amended under the following exceptional circumstances:-

- By specific agreement as formalised in the client's SLA; and
- By special request of organisation responsible for ICT implementation or regulation in Malawi and client management.

3.5.7. Data Archiving

All electronic data should be archived with the Department of National Archives.
No data should be destroyed without the written approval of the Department of National Archives.

3.6. ICT Audit

3.6.1. Preamble

In line with rapid advancement of technology most organisations have become increasingly reliant on computerised information systems to deliver public services and carry out their daily operations. As a consequence, the reliability, integrity and availability of computerised data and of the systems that process, maintain and report these data are a major concern to audit. ICT Auditors examine the adequacy of controls in information systems and related operations to ensure system effectiveness.

ICT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organisational goals to be achieved effectively, and uses resources efficiently.

ICT auditing is a branch of general auditing concerned with governance (control) of information and communications technologies (computers).

3.6.1.1 Controls in an ICT System

In order for any computer systems to work as they are designed, achieve results accurately, efficiently, and securely and perform within the specified constraints, they would need controls. These controls are of great value in any computerised system and it is an important task for an auditor to see that not only adequate controls exist, but that they also work effectively to ensure results and achieve objectives. Also controls should be commensurate with the risk assessed so as to reduce the impact of identified risks to acceptable levels.

Controls in a computerised information system reflect the policies, procedures, practices and organisational structures designed to provide reasonable assurance that objectives will be achieved.

Information system controls are broadly classified into two broad categories:

- General Controls
- Application controls

General controls include controls over data centre operations, system software acquisition and maintenance, access security, and application system development and maintenance. They create the environment in which the application systems and application controls operate. Examples include IT policies, standards, and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, service continuity planning, IT project management, etc.

Application controls pertain to specific computer applications. They include controls that help to ensure the proper authorisation, completeness, accuracy, and validity of transactions, maintenance, and other types of data input. Examples include system edit checks of the format of entered data to help prevent possible invalid input, system enforced transaction controls that prevent users from performing transactions that are not part of their normal duties, and the creation of detailed reports and transaction control totals that can be balanced by various units to the source data to ensure all transactions have been posted completely and accurately.

3.6.1.2 Objectives of ICT Controls

As a principle, the objectives of internal controls remain unchanged with the introduction of ICT. It is the control techniques that change with many of the manual controls being replaced with automated processes and new technical controls added to achieve the same objectives. Typical control objectives within a government ICT function are to ensure:

i. Provision of effective organisational control over functions related to the use of ICT infrastructure by clearly defining organisational objectives;

ii. Effective management control over development of ICT infrastructure resources in accordance organisational objectives;

iii. Operational management of ICT infrastructure in accordance with statutory requirements and industry good practices;

iv. Formulation of an adherence to policies, standards and procedures for all functions related to ICT infrastructure and

v. Efficiency and effectiveness of the ICT infrastructure systems towards achievement of its desired objectives.

3.6.1.3 Controls Based on Domains

Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organisation's sensitive information. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

Technical security controls (also called logical controls) are devices, processes, protocols, and other technology-based measures used to protect the C.I.A. of sensitive information.

Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorised employees access to the data centre do little good without some kind of physical access control.

3.6.1.4 Controls Based on Purpose

Directive security controls are the equivalent of administrative controls. Directive controls direct that some action be taken to protect sensitive organizational information. The directive can be in the form of a policy, procedure, or guideline.

Preventive – security controls that are put into place to prevent intentional or unintentional disclosure, alteration, or destruction of sensitive information. Notice that preventive controls may also cross-administrative, technical, and physical categories as discussed previously. The same is true for any of the controls discussed in this section.

Detective security controls have the function of providing an alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred, either manually or automatically. Example detective security controls are log monitoring and review, system audit, file integrity checkers, and motion detection.

Note that in some cases, Detective controls are complemented with a **Delay** mechanism – to prevent an attempt for unauthorised access from being able to progress immediately.

Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. Note that in many cases the corrective security control is triggered by a detective security control. A corrective control will essentially include **Assess** and **Respond** phases.

Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category.

3.6.1.5 Other Control Types

Deterrent security controls are controls that discourage security violations. For instance, “Unauthorized Access Prohibited” signage may deter a trespasser from entering an area. The presence of security cameras might deter an employee from stealing equipment. A policy that states access to servers is monitored could deter unauthorized access.

Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason (e.g. operational or technology constraints).

3.6.1.6 ICT Audit Standards

- ISACA COBIT v4.2 – COBIT (Control Objectives for IT) is a framework created by ISACA for information technology (IT) management and IT Governance. The framework provides good practices across a domain and process framework. The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate) and 34 processes in line with the responsibility areas of plan, build, run and monitor.

  The use of COBIT in any audit programme should be done sparingly – certain areas of COBIT should be selected to reflect the target organisation's maturity in ICT management and whether certain controls are indeed relevant for that organisation. A good start in using COBIT is in a maturity assessment process, where applicable controls are evaluated for its maturity and non-relevant controls are identified with suitable analysis. An auditor can then use this result to plan which areas of high risk should be focused for subsequent planning.
- ISO/IEC 27001:2005 Information Security Management – is the international standard for Information Security Management System and along with ISO/IEC 27002 (Guidelines) describes a complete framework of how information security management should be implemented in an organisation. The standard defines management and technical controls, the latter with sufficient detail (39 Control Objectives and 133 Controls). Organisations wishing to obtain a certification based on this standard may do so by appointing a suitable Certification Body to conduct a certification audit.
- ISO/IEC 20000:2005 IT Service Management – is the international standard for IT Service Management that describes how IT *as a service* should be managed. The ISO/IEC 2000x series provide a comprehensive definition of an IT Service Management framework and similar to the ISO/IEC 27001 standard, may be adopted for the purpose of obtaining an external Certification.

3.6.2. General ICT Audit Policy

1. ICT Audit aims to provide recommendations for improvements related to any control weaknesses.

2. ICT Audits can be conducted as a stand-alone activity or be part of a general audit.
3. The audit is based on a formal charter (audit charter). The Audit Charter shall contain at least:
    a. The purpose of the audit
    b. Scope of audit
    c. Authority of the auditors
    d. Auditors' Liability
    e. Auditors' responsibility
    f. Reporting of audit results
4. IT Audit shall be based on current Government of Malawi regulations on ICT and on the following standards and frameworks:
    - ISACA COBIT v4.2
    - ISO/IEC 27001:2005 Information Security Management
    - ISO/IEC 20000:2005 IT Service Management
5. Auditors should uphold professional and organizational ethics.
6. In all matters relating to audit activities, the audit unit should be independent and objective.
7. The auditor must have professional competence and ability to perform the tasks of information technology audit.
8. Auditors should prepare audit plans and procedures based on a risk-based approach. Results of risk assessments are to be used to set priorities and allocation of audit resources.
9. In the implementation of audit, the auditor should:
    a. Able to ensure the audit objective is achieved according to professional auditing standards;
    b. Gather sufficient evidence that can be trusted, and relevant to support its findings; and
    c. Document the audit process and audit evidence to support his conclusions.
10. Auditors shall also examine general IT controls for their performance (effectiveness and consistency). General controls include but are not limited to:

a. Policies and procedures for information and communication technology security;

b. Separation of duties;

c. Conformance to information system development policies (system development life cycle);

d. Changes to ICT environment and the change management process; and

e. Business continuity preparedness.

11. Meanwhile, the control applications include but are not limited to:

a. Identification, authentication, and authorization;

b. System interfaces;

c. Accuracy and completeness of transaction processing; and

d. Logging and audit trail.

12. If auditors find a weakness or inconsistency that is material in nature related to any controls, the auditor should communicate the issue to the appropriate level of management in a timely fashion.

13. Auditors must provide full and comprehensive report after the completion of audit process. This report must contain at least:

a. The purpose of the audit;

b. The scope of the audit;

c. The period of audit;

d. Audit findings, conclusions, and recommendations;

e. Limitations and constraints encountered in the audit process;

f. The procedure for distribution of reports according to the provisions of the Charter of the Audit.

14. Auditors may request assistance from external professionals to conduct the audit. Prior to employing external expert assistance the audit supervisor shall ensure that the outside personnel have the required skills, competence, professional qualifications, relevant experience, and independence.

15. After reporting the findings and recommendations, the auditor should monitor all findings to ensure audited implements corrective measures effectively.

3.6.3. General Guidelines

3.6.3.1 Audit of General Controls

The overall audit objective in reviewing the general controls is to ensure that the controls and procedures are adequate to provide secure, effective and efficient day-to-day operation of the ICT system. The controls and procedures, which together form the general controls, are discussed in the succeeding paragraphs.

3.6.3.2 Organisational controls

A fundamental aspect of any internal controls is the availability of sound organisational controls. Such controls are required to ensure that there is judicious separation of duties to reduce the risk of internal fraud or sabotage by limiting the scope of authority of any individual, there are comprehensive written standards and access to and use of ICT systems are properly authorised.

These high level controls are important as they influence the effectiveness of any lower level controls. Unless senior management of the organisation maintains and enforces appropriate ICT policies and standards, it is unlikely that other controls will be sufficiently strong to support a controls reliant audit approach.

An assessment of the high level ICT policies, strategies and procedures will provide the auditor with a reasonably reliable indication as to the existence and effectiveness of any lower level detailed controls.

3.6.3.2.1 Segregation of duties

The auditor should check whether adequate and effective segregation of duties has been in place amongst the staff operating the ICT systems as it substantially reduces the risk of error and fraud. Poor segregation could lead to any one person, with control over a complete processing function, making an error or committing a fraud without detection.

Evidence of separation of duties can be gained by obtaining copies of job descriptions, organisation charts and observing the activities of IT staff. Where systems use security profiles to enforce separation of duties, the auditor should review on-screen displays or printouts of employees' security profiles in relation to their functional responsibilities. Inadequate segregation of duties increases the risk of errors being made and remaining undetected; it also may lead to fraud and the adoption of inappropriate working practices.

In any major IT System the following IT duties should be adequately segregated:

- System design and programming
- System support
- Routine IT operations and administration

- System security
- Database administration.

A comprehensive Segregation of Duty Map can be seen in the following figure (Source: ISACA, USA).

Table 1: Segregation of Duty Conflict Matrix

	DBA Staging	DBA Production	System Administrator Staging	System Administrator Production	Manager	Software Developer	Security Officer	User
Uses Application	X	X	X	X	X	X	X	
Initiates Change			X		X			X
Authorises Change	X	X		X	X	X		
Tests Updates – Database		X		X	X	X	X	X
Tests Updates – Application	X	X	X	X	X	X	X	X
Implements Updates – Database	X		X	X	X	X	X	X
Implements Updates – Application	X	X				X	X	X
Access to Source Code		X		X	X		X	X
Administrative Access – Database O/S Staging		X	X	X	X	X		X
Administrative Access – Database O/S Production	X		X	X	X	X		X

Administrative Access – Application O/S Staging	X	X		X	X	X		X
Administrative Access – Application O/S Production	X	X	X			X		X
Administrative Access – Staging Database		X	X	X	X			X
Administrative Access – Staging Application	X	X		X	X			X
Administrative Access – Production Database	X		X	X	X	X		X
Administrative Access – Production Application	X	X	X			X		X
Monitors Changes and Security Events	X	X	X	X	X		X	X

Note: Cells marked with an "X" indicate roles and tasks that are incompatible with each other, and where segregation of duties is advised.

3.6.3.2.2 Physical Access Control

Physical access controls include controls against environmental threats, which operate across the whole ICT environment and affect all underlying systems. These controls are designed to protect the system hardware and software from damage, theft and unauthorised access. Restricting physical access to the ICT systems reduces the risk of unauthorised persons altering the financial information. During an audit, ICT Auditor should conduct assessment of physical access controls throughout the whole audit programme, by observations of how these controls are being implemented within areas/facilities under review, as well as by taking samples of control records.

3.6.3.2.3 Authorisation Control

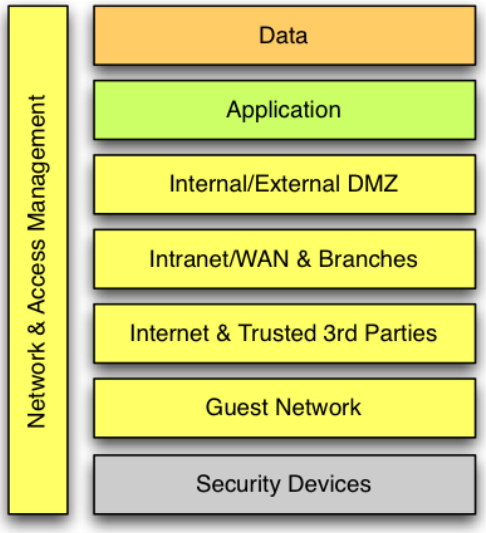
Authorisation control helps verify the identity and authority of the person involved in executing a procedure or an operation. This control is exercised through the use of passwords, signatures, smart cards, cryptographic systems etc. Such-controls ensure that only an authorised person has access to the system and its use, to enter and/or alter transactions, to take information etc.

In critical systems, authorisation controls may take the form of multiple layers of preventive (prior authorisation and verification of identity before issuing system access) and detective (regular review of user access), designed to provide a fail-safe mechanism. When auditing, it is important to analyse how a failure in one or more authorisation controls may affect the security of the system being protected.

3.6.3.2.4 Logical Access control

Logical Access controls are provided to protect the critical applications and underlying data files from unauthorised access, amendment or deletion. Logical access controls can exist at both an installation and application level. Controls within the general ICT environment restrict access to the operating system, system resources and applications, whilst the application level controls restrict user activities within individual applications.

Logical access controls can also be used to restrict the use of powerful systems utilities, such as file editors and system configuration panel. Logical access controls are often used with physical access controls to reduce the risk of the programs and data files being amended without authority. The importance of logical access controls is increased where physical access controls are less effective, for example, when systems make use of communication networks (LANs and WANs). The existence of adequate logical access security is particularly important where a client makes use of wide area networks and global facilities such as the Internet.



Implementation of layered controls should be defined based on access requirements and risks related to each access type. The figure above illustrates how various layer of controls should be applied logically to protect access from different user profiles.

The most common form of logical access control is login usernames followed by password authentication. For passwords to be effective there must be appropriate password policies and procedures, which are known to all staff and adhered to. Menu restrictions can be effective in controlling access to applications and system utilities.

Systems may be able to control access by identifying each individual user through their unique login ids and then having a pre-defined profile of authorised menus for each. The ICT Auditor should consider how easy it would be for users to 'break out' of the menu system and gain unauthorised access to the operating system or other applications. Some computer systems may be able to control user access to applications and data files by using file permissions. These ensure that only those users with the appropriate access rights can read, write, delete or execute files.

3.6.3.2.5 Change Management Controls

Change management controls are used to ensure that amendments to a system are properly authorised, tested, accepted and documented. Poor change controls could result in accidental or malicious changes to the software and data. Poorly designed changes could alter critical information, introduce system malfunction and remove audit trails. Audit should ensure that a new or amended system is thoroughly tested by its end users before operational implementation. These regular changes may be necessary to improve efficiency, functionality or remove programming faults ('bugs').

ICT Audit should emphasise that auditee organisations have an appropriate change management and configuration management controls. Configuration management procedures relate to the control of ICT assets and the subsequent update of records, whilst

change management relates to the authorisation, impact assessment, asset update, testing and implementation of changes.

3.6.3.2.6 Network Communication Security Controls

Network communication security controls are critical when LANs/WANs or web enabled systems are in use. Some important aspects to be covered by this control are as follows:

i. All sensitive information processed (transmitted) within the network should be protected by using appropriate techniques;
ii. Critical network devices such as routers, switches and modems should be protected from physical damage;
iii. Network configuration and inventories should be documented and maintained;
iv. Prior authorisation from Network Administrator should be obtained for making any changes to the network configuration.
v. Any changes made in the network configuration should be documented. The threat and risk assessment of the network due to these changes in the network configuration should be reviewed.
vi. The network operation should be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.
vii. Physical access to communications and network sites should be controlled and restricted.
viii. Communication and network systems should be controlled and restricted to authorised individuals.
ix. Network should be monitored using diagnostic tools by authorised personnel.
x. Network perimeter security should be used to isolate an organisation's data network from any external network. Networks that operate at varying security levels should be isolated from each other by appropriate firewalls. The internal network of the organisation should be physically and logically isolated from the Internet and any other external connection. All network security devices should be subjected to thorough testing for vulnerability prior to implementation and at least half-yearly thereafter. All web servers for access by Internet users should be isolated from other data and host servers.
xi. Connectivity with third parties should be implemented with suitable security controls. Organisations should establish procedures for allowing connectivity of their network or application system to any third parties. The permission to connect other networks and application system should be based on clear purpose (regulation, government policy) and approved by the Network Administrator and documented. All unused connections and network segments should be disconnected from active networks. Any systems accessing an organisation's host system must adhere to the general system security and access control guidelines. The suitability

of the protocol used for third party connections should be assessed prior to ensure compatibility and protection of data exchange. The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

xii. The responsibility of technically managing each system shall be allocated to a properly trained System Administrator, who is then responsible for operation, monitoring security and functioning of the system.

xiii. Any reports of unusual activity or pattern of access on the computer network should be investigated promptly by the Network Administrator. The system must include a mechanism for alerting the Network Administrator of possible breaches in security,

3.6.3.2.7 Business Continuity Planning

Each organisation should have an established plan to guard against disastrous events and ensure the continuity of public services (See related ICT Security Policies on Business Continuity Planning). The auditor should verify that there are adequate plans to resume processing in the event of complete failure of computer operations. The degree of continuity planning will depend on the size of the ICT department and the dependence of critical business processes on computer processing. Disaster recovery planning for ICT facilities should be treated as one element of an organisation's overall business continuity plan.

The extent of disaster recovery planning and the detailed measures required will vary considerably. Organisations with large ICT departments, with multiple business systems and complex communication networks may require comprehensive, up to date recovery plans which incorporate standby facilities at alternative sites.

Disaster recovery plans should be documented, periodically tested and updated as necessary. Untested plans may be satisfactory on paper but fail when put into practice.

Testing will reveal deficiencies and allow amendments to be made. The importance of adequate documentation is increased where significant reliance is placed on a few key members of the ICT department. The loss of key staff may adversely affect an organisation's ability to resume operations within a reasonable timeframe.

Back-up copies of systems software, mission critical applications and underlying data files should be taken regularly. Back-ups should be cycled through a number of generations by, for example, using daily, weekly, monthly and quarterly tapes. Back-ups should be stored, together with a copy of the disaster recovery plan and systems documentation, in an off-site fire-safe. Where end-user computing processes are used, in addition to centralised application systems, the auditor should ensure that there are also procedures for the backing-up of critical data stored on local hard disks.

3.6.3.3 Evaluation of General Controls

When reviewing general controls, the following areas should be covered:

i. Evaluation of ICT Asset management by acquiring a list of asset including, computers, ancillary and terminal equipment in use indicating model, performance details and verify the existence of this equipment – in many current implementation, a CMDB (Configuration Management Database) may be available for examination;

ii. Analysing ICT Management structure in the organisation by acquiring a current organisational chart and analyse how computing facilities are used/managed within the overall Organisation. The analysis should be extended to cover how the ICT Management structure is staffed by using up-to-date personnel chart of the ICT department showing the roles, responsibilities and authorities –ensure that all critical operational and governance roles are allocated;

iii. Examine whether operational procedures are in line with established practices by using the details of standards and operational guidelines that have been defined for each of the ICT functions, like data control, data preparation, system operation and verify that they have been implemented consistently. Also confirm that operational manuals are maintained and kept up-to-date, specifying the control procedures and whether they are enforced in practice through regular evaluations

iv. Verify the existence of the following terminal controls to protect data and system integrity:

   a. physical access controls to terminal rooms;

   b. user authentication controls through password protection and user directories;

   c. logging of terminal activities by all users.

v. Evaluate the effectiveness of physical security controls to protect against risk of man-made disasters. Examples of suitable controls are:

   a. Fire prevention controls (fire prevention steps, detection mechanism and firefighting arrangements);

   b. Regular maintenance of computer and related equipment;

   c. Environmental control system (air conditioning) and protection against possible radiations, vibrations;

   d. Human resource controls for possible industrial action, malicious action by programmers, operators, and temporary staff;

   e. Security awareness and training programmes provided to all employees;

   f. Emergency shut-down procedures in case of power failures;

   g. Chain of custody of software, data files and tape library;

   h. Adequacy of back-up files (offsite storage included);

   i. Restricting operator access to program files and data;

j. Procedures for reconstructing files in the event of loss or disk errors/tape errors(contingency plans);

k. Back-up for computer equipment failure through the use of compatible equipment at other dispersed sites;

l. Data Centres, Server Rooms and Data Communication Rooms should be off limits to all except systems operators, hardware engineers and

m. Insurance policy of the installation to cover possible risk (if available).

3.6.3.4 Application Controls

Application control mechanisms are largely specific to an application and have a direct impact on the way individual transactions is processed. These controls are implemented to provide assurance that all transactions are authorised, valid and recorded. Since application controls are closely related to individual transactions the audit will provide the auditor with assurance as to the level of accuracy of a particular data file.

Prior to conducting and evaluation of application controls, it will be necessary to ensure a suitable understanding of the application system;

i. The business process done through the application, including inputs, outputs and interfaces with other processes/systems;

ii. How data is to be managed within the applications, including volume of transactions and data stored;

iii. Technology platforms used and how they are configured.

3.6.3.4.1 Audit Requirements

When auditing an ICT infrastructure that are complex or involving multiple technology platforms, the auditor shall identify pre-requisite conditions to ensure that the system can be audited in an effective and efficient manner. Audit trail has to be made available to enable tracing of an item from input through to its final destination and break up a result into its constituent parts. (In many cases, auditors may have to use audit software or test data for the efficient execution of their audit. They have, therefore, to seek reasonable requests for the access to copies of system data files, report generators and processing time).

Deriving the audit requirements for a system under development will involve collecting information on the existing system:

i. Weaknesses in the current system affecting the audit approach,

ii. Features in the existing system, which are relied on to provide an effective audit, that should be retained in the new system, and

iii. Additional facilities, not currently provided in the existing system, which would assist the audit of the new system.

3.6.3.4.2 Controls Mechanisms

As a minimum, audit of an application system being used for operational transactions involves verification of input/output controls, processing controls and audit trail. Evidence of audit to allow a reasonable conclusion on the existence of controls and their adequacy may be obtained in the following areas:

i. Whether the data processed are real, complete, accurate and not provisional?
ii. Whether expected output is produced and disseminated on time?
iii. Whether application programs process the data as intended and accurately?
iv. Whether a complete audit trail is available for tracing back a transaction from the final result to the initial input?
v. Whether the data and changes to it are authorised by appropriate authority both in the user and computer departments?
vi. Whether paper trail related to input data are maintained and what is the extent of compliance?
vii. Whether there is a preliminary check on input data to ensure completeness?
viii. Whether the application system provides for the following programmed controls:
    a. Check for missing/duplicate transactions;
    b. Controls on rejected items and keeping them under computer suspense;
    c. Input validation for data format (alpha-numeric checks to conform to data types);
    d. Limit/range checks for each data format;
    e. Overflow checks;
    f. Non-blanks or zeros fields (mandatory fields);
    g. Check digits;
    h. Compatibility checks;
    i. Exception condition check;
    j. Total for a batch/lot;
    k. Record totals and summaries for reconciliation
ix. Whether output reports are test-checked before being distributed to user departments and the output is produced in accordance with a prescribed schedule.

3.6.3.4.3 Audit Trail

The objective of an audit trail is to obtain sufficient evidence on the reliability and integrity of the application system. To achieve this, the audit trail should contain enough information to allow management, the auditor and the user:

i. to reconstruct all complete/incomplete/erroneous processes;
ii. to verify summary totals and
iii. to trace the sources of intentional and unintentional errors.

The audit trail should include the following information:

- System information including time stamps of start-up, stop, restarts, recovery etc.

- Transaction information including input events that result in change to the database, control totals and rejected items (relevant to database applications).
- Information related to user activities including terminal log-on/off, password use, security violation, network changes and transmission statistics (relevant to transaction processing).

In general, the audit trail of an application system may not always be evident when compared to a manual system, since data are often retained in magnetic media and output is limited to a small number of total items processed, with reports produced only on exception basis. If the design of the application system does not provide for adequate audit trail this should be brought out in audit review, highlighting control weaknesses or lack of controls in the system. Apart from errors that might creep into the system, there is a possibility of frauds, which might occur due to undetected control weaknesses

3.6.4. Audit Methodology

3.6.4.1 Types of ICT Audits

An audit programme is usually developed for particular reason – this can be an annual audit to cover the entire organisation, or specific audit conducted to focus on certain issues of interest. The former is clearly of such magnitude that audit units usually derive an annual audit programme to allow wide-ranging areas to be covered so as to provide overall status of compliance to management.

In most cases, the annual programme will have to include specific in-depth audit to be done on certain initiatives that may be related to on-going strategic initiatives or to examine level of compliance to new regulations. For reference, the following types of ICT audits may be used singly or in multiple combinations, to help define an audit programme:

- Operational computer system/network audits: review the controls within and surrounding operational computer systems and networks, at various levels e.g. network, operating system, layered software, application software, databases, logical/procedural controls, preventive/detective/corrective controls, crypto, system logging.
- ICT installation audits: examine the physical aspect of the computer building, server rooms, network/communication cupboard, including aspects such as physical security (walls, CCTV, locks, guards, barbed wire, visitor procedures), environmental controls (fire and flood protection, power supply, air conditioning), computer and network operations processes and management systems.
- Systems development audits: typically cover either or both of two aspects: (1) project or programme management controls); and (2) the specification, development, testing, implementation (installation and configuration) and initial operation of technical and procedural controls, including classical technical information security controls and the related business process controls such as divisions of responsibility. See further discussion on this below.

- ICT management audits: review the organization, structure, strategy, work planning, resource planning, budgeting, cost controls etc. and, where applicable, relationships with outsourced ICT providers.
- ICT process audits: review the processes which take place within IT department such as application development, testing, implementation, operations, maintenance, housekeeping (backups, preventive maintenance etc.), support, incident handling.
- Change management audits: review the planning and control of changes to systems, networks, applications, processes, facilities etc., including configuration management, control over the movement of code from development through testing to production, and the management of changes to the organisation as a result of ICT.
- Information security & control audits: review controls relating to confidentiality, integrity and availability of systems and data.
- ICT legal compliance audits: review legal and regulatory aspects of IT systems (e.g. software copyright compliance, protection of personal data).
- Certification and other compliance audits: compliance audit based on information security standards such as ISO/IEC 27001 and industry standards such as PCI-DSS. Formal certification audits typically have strictly defined scopes.
- Disaster contingency, business continuity planning and IT disaster recovery audits: review arrangements to restore some semblance of normality after a disaster affecting the IT systems, and perhaps assess the organisation's approach to risk management, reviewing the links between (a) identifying and protecting critical business processes, and (b) securing the supporting IT services, systems, network and processes. These audits may or may not cover the much-neglected but vital issue of resilience, which is of course all about avoiding disastrous outages as far as possible.
- "Special investigations": contingency and other un-pre-planned iaudit such as investigating suspected frauds or information security breaches, performing due diligence review of IT assets for mergers and acquisitions etc.

3.6.4.2 Preliminary evaluation

The first step in audit should be preliminary evaluation of the ICT infrastructure covering:

i. how the ICT function within the organisation is managed.
ii. use of ICT infrastructure and related facilities,
iii. applications processed by the computer and their relative significance to the organization and
iv. methods and procedures laid down for implementation of new applications or revision to existing applications.

In the course of a preliminary evaluation, the auditor should ascertain the level of control awareness in the auditee Organisation and existence (or non-existence) of control standards. The preliminary evaluation should identify additional potential key controls for further improvement and any serious key control weaknesses. For each control objective

the auditor should state whether or not the objective has been achieved; if not, he should assess the significance and risks involved with due to control deficiencies.

3.6.4.3 Audit Techniques

After completing the preliminary evaluation of the computer systems, the auditor has to decide on the appropriate audit approach, system based or direct substantive testing. In doing so, the aspects to bear in mind are:

i. results of the preliminary evaluation;
ii. possible lack of any audit trail and the practicability of testing;
iii. effective compliance testing of key computer controls (which may be difficult) and testing a complex control may require large samples.

3.6.4.4 Direct Substantive Testing

If Direct Substantive Testing approach is chosen, a sample of transactions should be selected and tested. Result of the preliminary evaluation will be of help particularly as it would have:

i. provided an overall assessment of the control environment and identified any serious weaknesses which should be raised with the auditee,
ii. given sufficient familiarity with the system to be able to decide the point from which to select the transactions for testing and how to substantiate them efficiently.

3.6.4.5 Systems Based Audit

For System Based Audit approach, aspects of regularity, economy, efficiency and effectiveness of the system have to be looked into besides evaluating data integrity, and data security as explained below:

i. System effectiveness is measured by determining whether the system performs the intended functions and whether users get the needed information, in the right form when required;
ii. A system is economical and efficient if it uses the minimum number of information resources to achieve the output required by the users. The use of system resources - hardware, software, personnel and money - should be optimized;
iii. System activities would be regular if they comply with applicable laws, rules, policies, guidelines etc;
iv. Achieving data integrity implies that the internal controls must be adequate to ensure that error are not introduced when entering, communicating, processing, storing or reporting data; and
v. Data system resources, like other assets, must be sufficiently protected against theft, waste, fraud, unauthorized use and natural disasters.

The key controls for ensuring the above will have to be identified, recorded, evaluated and compliance tested. The result of the preliminary evaluation would be of help particularly as they would indicate system deficiencies, major weaknesses and the areas requiring in-

depth study. Identification of key controls would also depend on experience of the auditor gained in course of audit of similar installations.

3.6.4.6 Computer-Aided Audit Techniques

Computer-Aided Audit Techniques refer to the use of computers, including software, as a tool to independently test computer data of audit interest. Some well-established techniques are:

i. collecting and processing a set of test data that reflects all the variants of data and errors which can arise in an application system at different times;
ii. using integrated test facilities, built into the system by the auditee to help the auditor in his requirements, as one of the users of the system;
iii. simulating the auditee's application programs using audit software to verify the results of processing;
iv. reviewing program listings periodically to see that there are no unauthorised alterations to the programs;
v. using either commercial software or in-house developed programs to interrogate and retrieve data applying selection criteria and to perform calculations and
vi. extracting samples of data from the auditee database/files, using sampling techniques, for post analysis and review.

The particular computer audit technique employed depends on:

i. the type of application system under review;
ii. the extent of testing required;
iii. the availability of resources in terms of computer facilities, and the level of skills among the audit staff; and
iv. Volume of data and availability of printed information.

Where data volume is small and adequate printed information is available to carry out a meaningful clerical audit, there is no need to employ computer techniques, which are costly and time consuming. To elaborate further, the auditor should break up his project of application system audit into three stages. In the first stage, he will carry out the examination of audit trails, intermediate printouts as required, system logs and operational controls. As a result of audit in the first stage, if the auditor feels that the adequacy of controls requires further verifications, in the second stage he can carry out compliance testing by using integrated test facilities with resident audit programs. If the compliance testing exposes some control weaknesses, substantive testing may be resorted to in the third and final stage using retrieval software and simulation techniques with audit software.

Today, many DBMSs have built-in query and report writer facilities. Unstructured queries on the data files are also possible in some advanced systems. These utilities could be profitably employed for audit purposes. Good software architecture should include an audit module, specifically designed to allow secure audit processes to be done within the application by authorised personnel.

3.6.4.7 Auditing System Procurement and Development

3.6.4.7.1 Audit of System Procurement

Generally the procurement of ICT facilities involves the following stages:

i. Definition of an ICT policy and strategy (evaluation of organisational requirements and the ways or means of satisfying them);
ii. Establishing the need and defining it as formal initiative;
iii. A thorough examination and evaluation of the alternative courses of action available;
iv. Specifying precisely the requirements (delineating existing and future applications, hardware, software, modes of operations, conditions of supply, etc.);
v. Evaluating the alternative sources of supply and selecting the most appropriate source(s), and;
vi. Physically acquiring the facilities and the systems.

Often these stages overlap or merge imperceptibly, into one another. Acquisition of ICT system may include both hardware and software components, either procured separately, or integrated as a turnkey project.

An audit of an ICT procurement project has to review the adequacy of administrative procedures and controls used by the organisation when considering and deciding upon the acquisition of ICT facilities. For this purpose, the audit has to ensure that:

i. a sound administrative structure exists to produce a proper analysis of the requirements of ICT facilities:
ii. feasibility study and internal project report containing proposals, costs and benefits to provide management with unbiased reference for decision making;
iii. specifications of requirements for acquisition, enhancement or replacement of computing facilities are stated concisely and precisely (as they form the basis of submitting commercial proposal for potential suppliers);
iv. equipment selection justification for any specific hardware and software;
v. the process of evaluation and selection ensure that the requirements of the Organisation are met in the most effective and efficient way;
vi. both technical and commercial aspects of the proposal are evaluated according to standard contracting procedures;
vii. procurement action is taken after ensuring that the suppliers' offers meet the requirements of the specifications by taking into account of the following:
    a. technology options available at the time of procurement,
    b. useful life of the asset,
    c. incidental costs which could eventually be of sufficient magnitude, besides hardware and software costs and
    d. future development plans of the potential suppliers in terms of expendability, upgradability, etc.

viii. installation of equipment and adequacy of testing and post implementation review and costs are conducted to ensure original requirements are met.

3.6.4.7.2 Audit of System Development

Since the underlying purpose of acquisition and development (designing, building or modifying) of an ICT system is essentially the same, the audit concerns are equally important in the review of systems development. In essence, the audit objective of system development controls is to ascertain that procedures are adequate to ensure that the development results in well-documented systems incorporating adequate controls and meeting properly defined user requirements in an efficient manner.

Where systems development is entrusted to third party contractors, the contract and its management become important audit concerns. It should be ensured that the vendor provides complete documentation along with source code, where this is possible or economically viable. Further, the terms and conditions like the rights over the source code provisions for modifications/updating in future should be examined. The auditors should analyse any provisions in cases of non-delivery of services or other non-adherence to contractual obligations.

In general, system development audits can be categorised into three general types:

i. monitoring audits, in which the auditor evaluates the project throughout the process to determine whether development is proceeding effectively, e.g., whether interim milestones are being met, expenditure rates are as predicted, high quality documentation is being written, software conforms to established. technical standards, tests are being conducted as scheduled or evaluated as planned;
ii. design review audits, in which the objective is to determine whether the preliminary and detailed designs accurately reflect the functional data and systems specifications, and incorporate adequate internal controls and
iii. post implementation audits, performed three to six months after the system becomes operational, serve to evaluate whether the system meets requirements, is cost-effective and generally provides benefits predicted in project planning documents.

The ultimate responsibility for incorporating internal controls and an adequate trail into computer-based systems must rest with the auditee. The auditor therefore does not need to provide, as a matter of policy, any consultancy advice on developing systems. Nonetheless, audit should be aware of all system developments, which are likely to have significant impact on his audit.

When auditing a system under development, it is important for the auditor not to be drawn into unproductive involvement in system development. Some of the more important points that should be examined are the following:

i. Whether a published standard methodology is being used for designing and developing systems?

ii. Whether there is a common understanding by all parties-users, systems analysts, management and auditors-of the basic structure of both manual and computer processing activities, as well as of the concepts and needs for control and of the applicable control techniques? (This understanding must be reached first at a non-technical, user level)

iii. Who authorises ICT applications development – the user or steering Committee or management?

iv. Whether project management techniques, are applied in system development work – that is to say, are there project decision milestones, time and cost estimates so that progress could be monitored against estimates?

v. Whether programming standards using modular structured methodology are being adhered to in coding?

vi. Whether existing in-house or external available application packages were considered before deciding upon new in-house application development?

3.7. ICT Project Management

3.7.1. Purpose

This standard provides an overview of the essential components of the project management methodology used within the organisation.

This standard includes the 'what', 'when' and 'why' of project management methodology. Examples of 'how' can be found in supporting procedures and forms.

As a methodology, this standard provides a structured approach to managing projects with ICT components.

3.7.2. Definitions

For the purposes of the Project Standards and Guidelines and all associated and related documentation and processes, the following terms are defined:

Acceptance testing	Formal testing conducted to determine whether or not a system satisfies its pre-defined acceptance criteria, and to enable the client to determine whether or not to accept the system.
Accepted	The recorded decision or formal sign off by the client, that an output or sub-output has satisfied the documented requirements and may be delivered or used in the next part of the process.
Assumptions	Assumptions are factors that, for planning purposes, are considered to be true, real or certain.
Authorised	The recorded decision that a deliverable or output has been cleared for use or action after having satisfied quality standards for the project.
Baseline metrics	A set of indicators against which performance may be judged and reported.
Business Owner	The main clients of the project who are responsible for using the project outputs and realising the agreed project outcomes/benefits.
Clients	Those who will use the project outputs, and will generate the targeted outcomes (benefits).
Constraints	Factors that will limit options (e.g. budget, deadlines, technology, scope or legislative processes.)
Cost Benefit Analysis	The economic and business justification for a proposed project.
Deliverable	A tangible, verifiable work output such as a mandate, a detailed

	project plan, any report, manual, specification, programming, or other output developed as part of a project.
GOM	Government of Malawi
Governance	The management structure created for the life of a project.
Department of E-Government	Organisation responsible for ICT implementation in Malawi of the Government of Malawi.
Issue	A concern that needs to be addressed, either immediately or during the project.
Key elements	Essential aspects of managing projects that must be considered, no matter the project size or complexity.
Key stakeholder	An individual or group whose interest in the project must be recognised if the project is to be successful. In particular, those who may be positively or negatively affected during the project or on successful completion of the project.
Milestone	A significant scheduled event that acts as a progress marker in the life of a project.
Non-key stakeholder	Stakeholders who do not need to be recognised in order for the project to be successful, but who will be identified as a result of the process of identifying all stakeholders.
Outcome(s)	The benefits and other long-term changes sought from undertaking a project.
Output(s)	The services or products delivered to the Business Owner(s) by the project.
Performance measures	Criteria for measuring a project's success, whether the project is under control; and the level of adherence to documented plans, methodologies, and standards.
Phase	A section of work for which there are no measurable outcomes at the end, although some outputs may be produced.
Risk	Any factor (or threat) that may adversely affect the successful completion of the project.
Scope	A clear statement of the areas of impact and boundaries of the project, including the target outcomes, clients, outputs, work and resources (both financial and human).
Scope creep	Any modification to the scope of a project that has not been authorised or approved by the appropriate individual or group.

Stakeholder	A person or organisation that has an interest in the project processes, outputs or outcomes.
Target outcome(s)	The measurable benefits that are sought from undertaking a project. Target outcomes are achieved from the use of the outputs delivered by a project.
Test plan	A detailed plan that addresses all aspects related to the test of an output or sub-output.
Test specification	Describes the test criteria and the methods to be used in a specific test to assure the performance and design specifications have been satisfied. The test specification identifies the capabilities or program functions to be tested and identifies the test environment. It may include test data to support identified test scenarios.
Version control	A control or identification system for documents, outputs and sub-outputs, enabling stakeholders to readily identify each different release.
Stage	A major segment of a project for which there are outputs and outcomes at the end.

3.7.3. Scope

Most of the principles that apply to significant (medium to large) projects also apply to smaller projects. However, the extent to which these principles are applied will vary, depending on the complexity of the project.

A scaled down version of these standards and guidelines may be adopted to support the management of smaller projects.

The procedure: *Determining a Project Size* will assist in determining both the size of a project (small, medium or large) and the amount and type of documentation to be developed for each project size.

3.7.4. Guides, Procedures, Worksheets and Forms

The guides and procedures, standard templates and forms for use in implementing these standards and guidelines are those provided by Prince2 Project Management methodology.

3.7.5. Project Management

3.7.5.1 Definition

A project involves a group of inter-related activities that are planned and then executed in a certain sequence to create a unique product or service within a specific time frame.

Projects are often critical components of an organisation's business strategy, or relate directly to policies and initiatives of the organisation.

Projects vary in size or complexity, for example they may:

- involve changes to existing systems, policies, legislation and/or procedures
- entail organisational change
- involve a single person, or many people
- involve a single unit of the organisation, or may cross organisational boundaries
- involve engagement and management of external resources
- cost anywhere from $1,000 to more than a $1million
- require less than 100 hours or take several years.

3.7.5.2 Essential characteristics

A GOM ICT project is characterised as having:

- Business Case
- definable, measurable project outcomes that relate to GOM goals
- project outputs (required for the attainment of the project outcomes) produced by a project team(s)
- project governance structure
- well-defined project team(s)
- criteria to measure project performance.

The structure of a project will vary, depending on the benefits the project is intended to provide. To achieve these benefits, a project may need to be structured into a number of sub-projects.

3.7.5.3 Project management

Project management is the formalised and structured method of managing change. Project management focuses on achieving specifically defined outputs in a certain time, to a defined quality, and with a given level of resources, in order that specific outcomes are achieved.

Effective project management is essential for the success of a project.

The GOM advises adoption of the PRINCE2 Project management methodology.

3.8. Systems Development

3.8.1. Purpose

This standard defines what controls will be implemented by organisations in relation to System Development and Maintenance.

This standard is consistent with, and should be read in conjunction with the Information Systems Security Guidelines.

This standard interprets current industry standards and recommends an application development standard for adoption in the Malawi for the software/application development lifecycle, consistent with enterprise architecture standards (in particular, compliance with the enterprise architecture checklist), principles, and best practices.

The application development standard will provide:

- Adequate Application Development Standards for all stages of the application development process
- Minimum requirements for application development activities, deliverables and acceptance sign-off
- A general measure for ensuring the application development methodology is in compliance with the application development standard.

3.8.1.1 Application of the standards

Each project will have different requirements and it is up to individual project teams to determine whether they will take a 'pure' or 'hybrid' approach combining aspects of various standards. Teams may adopt a hybrid standard if they think it will better serve the needs of the project, as long as the methodology is fully articulated and adhered to. The systems development standards are divided into the following.

3.8.1.2 Programming Standards

Project Teams are expected to maintain standards for the development of the application/software source code. Their purpose is to increase application/software quality, by proper commenting, limiting module complexity, systematic naming conventions, and other techniques. Such standards are often dependent on the choice of programming language.

3.8.1.3 Design Standards

Project Teams will also benefit from design standards. These can help ensure that consistent techniques are used, e.g. in conjunction with object-oriented design methods. Guiding principles, such as encapsulation and information hiding, may be defined, and checklists maybe developed for use in the design reviews.

3.8.1.4 Applicability statement

Government of Malawi IT Standards apply for use by all Project Teams. As new GOM ICT standards are approved, they are deemed mandatory on a go-forward basis (Go-forward basis means at the next available project development or procurement opportunity).

3.8.1.5 Requirement Levels

Within this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

Must	This requirement is not optional
May	The implementer *may* choose to take one or more of a selection of options, but *must* make a choice of one or more, as dictated within the context of the item
Should	The implementer *must* choose this action, *unless* business functionality dictates otherwise. Exceptions *must* be approved by management, as modifications to the standard practice

3.8.2. Application Development in an Organisation

While various application development methodologies have been developed to guide application development processes, the key application development methodologies used within the organisation are Waterfall and Iterative. Generally, the critical objectives, activities and deliverables of each of these methodologies remain the same. Organisation responsible for ICT implementation in Malawi has undertaken the task to identify these various SDLC, and develop an application development standard that is applicable across various methodologies. Project Teams will use this standard to help guide application development in a consistent, standard and predictable manner.

Effective application development processes are critical to the success of IT projects. Project Teams must select and follow one of the application development processes that can be categorized as Waterfall or Iterative; however, this System Development Standard must be used within the organisation to achieve compliance. This standard clearly defines expected application development activities, measures and deliverables for each phase to help in ensuring that the necessary standards are maintained through the entire life of the project.

PROJECT TEAMS MUST SELECT ONE APPLICATION DEVELOPMENT METHODOLOGY AND USE IT FOR THE DURATION OF THE ENTIRE PROJECT.

3.8.2.1 Waterfall SDLC

The waterfall model is a popular version of the software development life cycle model for software engineering. Often considered the classic approach to the application/software

development life cycle, the waterfall model describes a linear and sequential development method with distinct goals for each phase of development.

3.8.2.2 Iterative Incremental SDLC

Iterative and Incremental Development is an application/software development process developed in response to specific weaknesses of the more traditional waterfall model.

The iterative process starts with architecturally significant subset of the application/software requirements (often the high risk requirements) and iteratively enhances the evolving sequence of versions until the full application/software is implemented. At each iteration, design modifications are made and new functional capabilities are added. This allows the project team to take advantage of what was learned during the development of earlier, incremental, deliverable versions of the application/software. The product is defined as completed when it satisfies all of its requirements.

3.8.3. Application Development Standard

Application development shall follow the Waterfall model and the Iterative Incremental models. Team members may choose to use a hybrid of these models and other modern development methodologies.

3.9. E-Waste Management

3.9.1. Preamble

The *GOM ICT Standard for e-Waste* covers the collection and handling of waste ICT electronic equipment within the Government, taking into account appropriate environmental and sustainability factors.

For the purposes of this standard, electronic waste or e-Waste may be defined as all desktop computers, notebook or laptop computers, CD-ROM and DVD equipment, data projectors, digital cameras, telephones, mobile phones and personal digital assistants (PDAs), printers, photocopiers, fax machines and multifunction devices (MFDs), keyboards and similar peripheral ICT devices, servers, hubs, switches, bridges, routers, power supplies and batteries, UPS, scanners, electronic entertainment devices and consoles, and other similar items. This definition includes used electronic equipment destined for reuse, resale, salvage, recycling, or disposal. E-Waste is considered as waste at the point that the Government permanently discards the item of equipment from its ownership. The following principles will apply to the responsible disposal of e-Waste:

- Disposal, Data protection and Information integrity; and
- Environmental protection and Social responsibility.

The coordination of activities associated with the appropriate handling and disposal of e-Waste will be managed by organisation responsible for ICT implementation in Malawi ICT Common Services Division. Records will be maintained to document the amount of e-Waste disposed of each year in accordance with reporting requirements demonstrating compliance with environmentally friendly initiatives.

3.9.2. Standards

3*.9.2.1 Disposal, Data Protection and Information Integrity*

Disposal of Government ICT assets and equipment, deemed as e-Waste, will be in accordance with procedures specified in these Standards. Coordinated e-Waste disposal will be scheduled at organisation responsible for ICT implementation in Malawi headquarters semi-annually and as required at other locations outside Lilongwe. Organisation responsible for ICT implementation or regulation in Malawi will make every effort to ensure maximum usage and value for money is obtained from all electronic items to ensure that e-Waste is minimised.

Only designated collection and disposal points will be used for e-Waste. NO electronic equipment and e-Waste will be placed in general refuse bins located on Government of Malawi property. Procedures for the safe handling and disposal of e-Waste will be available to the public.

Equipment that is to be disposed may hold sensitive information and licensed software applications. Provisions within the *GOM Standard for ICT Information Management and Security* and the associated *GOM ICT Standard for Information Asset Classification and Control* will be followed to ensure that any personal or sensitive information has been removed from electronic storage media or such media is rendered unreadable and/or unusable. Where ownership of the equipment is to be transferred to a third party with the intention that the third party will continue to use the equipment, Organisation responsible for ICT implementation or regulation in Malawi staff will ensure that the equipment only contains licensed software applications and operating systems that can be legally transferred with the equipment.

3.9.2.2 Environmental Protection and Social Responsibility

The Government will not dispose of electronic equipment that is within its agreed lifecycle and continues to be supported by vendors under appropriate maintenance and warranty support agreements. E-Waste equipment shall be disposed of or recycled in an environmentally and socially friendly manner in accordance with the National Environmental Act. Organisation responsible for ICT implementation in Malawi will make all reasonable efforts to ensure that e-Waste equipment does not end up in landfills in Malawi and is not exported to end as landfill in the destination country.

3.9.2.3 ICT Procurement

The acquisition of environmentally preferable or 'green" goods and services is a key priority of organisation responsible for ICT implementation in Malawi ICT Common Services Division, and the Division will consider selection criteria for ICT goods and services that have a lower impact on the environment and the health and well-being of staff and the community and will be ethically and socially responsible when considering value for money.

3.9.3. User Education

The responsible disposal of e-Waste will become an important issue as ICT equipment usage continues to grow. Most staff are not fully aware of the range of hazardous materials used in the manufacture of ICT equipment and the requirement for special disposal of such equipment so that adverse environmental damage does not occur. Most staff and members of the wider community are becoming more environmentally conscious and will recycle and dispose of ICT equipment responsibly if they have appropriate information.

Addressing the responsible removal of e-Waste and recycling requires user education programmes to be incorporated into staff induction and development activities to ensure that it becomes part of the culture at GOM. Organisation responsible for ICT implementation in Malawi ICT Common Services Division will develop material and education programs that will be published on organisation responsible for ICT

implementation in Malawi website and delivered in person to all staff during basic ICT training sessions.

3.10. Strategic and Operational Planning

3.10.1. Preamble

This standard is intended to identify the various processes and activities performed within the Government/Organization that influence the allocation of ICT resources towards ensuring projects and activities are aligned to achieving the business requirements of the Government/Organization.

This standard has been put in place to ensure that ICT strategic and operational planning is consistent with the management and direction for ICT investment and assets within the Government/Organization. When performing ICT strategic and operational planning, the Government/Organization has implemented processes to ensure that ICT goals and objectives are aligned with the Government/Organization business priorities and plans. To this end, the Government/Organization is continuously improving the collection of information related to the Government/Organization ICT environment to assist and ensure that informed decision-making can occur and that optimisation of ICT resources is encouraged.

3.10.2. The ICT Planning Framework

3.10.2.1 How ICT Planning is aligned

The Government/Organization should establish a range of processes and procedures to ensure that the existing and future ICT resources, strategies and plans remain current and up-to-date. The review, assessment and prioritisation of Government/Organization ICT strategies and plans should be undertaken annually by a range of interested stakeholder groups.

The ICT Unit in organisation responsible for ICT implementation in Malawi has an integral contributor to the Government/Organization planning framework. The ICT Unit in organisation responsible for ICT implementation in Malawi has implemented a consolidated information technology support model and service delivery interfaces to assist ICT management align future planning and decision-making with business requirements. Concomitant with this, the ICT Common Services Unit in organisation responsible for ICT implementation in Malawi has implemented relationships with a range of stakeholders to ensure that ICT strategic and operational planning is based on informed discussion and input from a range of interested parties and is therefore more likely to result in successful outcomes. Individual key components of this model include:

Governance Structure

- ICT Steering Committee
- Ad-hoc ICT Business Advisory Committees (appointed by the CIO)
- Ad-hoc User Reference Groups (appointed by the CIO)
- Ad-hoc Technical Working Groups (appointed by the CIO)

Service Delivery Interface

- ICT Divisional Charter
- Products and Services Catalogue
- Relationship Management
- Service Level Agreements

Utilising the resources of these individuals and groups, ICT management is better prepared to contribute to the Government Planning Framework.

3.10.2.1.1 Organisation responsible for ICT implementation or regulation in Malawi's ICT Common Services Divisional Charter

Organisation responsible for ICT implementation in Malawi ICT Common Services Division Charter is reviewed annually to ensure it is aligned to the vision and mission of the Government and maintains its currency according to divisional philosophy and environmental changes.

3.10.2.1.2 Products and Services Catalogue

The Products and Services Catalogue is an overview of services provided by the ICT Common Services Unit, informs of service availability and how services are provided.

3.10.2.1.3 Relationship Management

The aim of relationship management is to monitor and improve the delivery of products and services to clients and maximise the organisational value and return of investment of the products and services portfolio. Relationship Management framework operates at two or three levels where levels two and three may be combined.

1. Level One Strategic – Meetings and linkages between the CTO and senior GOM/Organization Executives.
2. Level Two Tactical – Meetings and networking between Organisation responsible for ICT implementation or regulation in Malawi Managers and Organisational Managers with appropriate representatives from the client organisation.
3. Level Three Operational – Meetings between Managers and ICT staff to report on the SLA performance against the targets and identifies initiatives to enhance achievement of performance and/or improve the relationship.

3.10.2.1.4 Service Level Agreements

The ICT Common Services Unit underpins the services it provides through Service Level Agreements which list the core services that will be provided and a matrix of key performance indicators, reporting structures responsibilities, and critical service dependencies. There are three categories of agreement as follows:

1. Core Desktop SLA
2. GWAN SLA – for government entities

3. Product SLA

SLAs are signed off by the ICT Common Services Unit and the Service Receiver and reviewed annually.

3.10.2.2 ICT Planning Details for Malawi Civil Service

ICT Common Services Unit management adheres to the planning timetable designated by the Malawi Civil Service ICT Policy and schedules ICT planning activities and input to coincide with this timetable. ICT management contribute to the following:

- GOM ICT Strategic Plan (5 year timeframe).
- Individual GOM Ministry/Department (Organisational) Strategic Plans (3 year timeframe).
- Organisation responsible for ICT implementation or regulation in Malawi Strategic Plan (3 year timeframe).
- ICT Operational Plan (1 year timeframe).
- Organisational ICT Resource Management Plan (ORMP) (1 year timeframe).
- ICT Capital Investment Plan (3 year timeframe).
- Government ICT Enterprise Architecture (ongoing).

ICT Executive Managers Workshops

Three one-day workshops involving the ICT Executive Management Team (Director, CTO, GWAN Service Manager, and ICT Common Services Unit Manager, of Organisation responsible for ICT implementation or regulation in Malawi), and all other Organisation responsible for ICT implementation or regulation in Malawi ICT Managers shall be scheduled each year. The focus of these workshops shall be to discuss planning initiatives and activities.

The focus of the meeting will be:

- to review the ICT Operational Plan for the preceding year and assess opportunities for improvement.
- to review the ICT Divisional 3 Year Plan.
- to confirm the coming years ICT Operational Plan.

Organisation responsible for ICT implementation or regulation in Malawi Plan (3 year timeframe)

The ICT Divisional Plan is strategic in nature and is designed to identify how the Divisional goals are aligned to the Organisational Goals enunciated in the GOM/Organization ICT Strategic Plan.

For each Organisational Goal, the Division identifies:

- the goal that will be activated,
- the strategies in support of this Goal,

- the outcomes that are expect to achieve, and
- the success indicators that will be monitored to inform how progress is being made related to achievement of the Goal and Strategies.

ICT Operational Plan (1 year timeframe)

The ICT Operational Plan is more immediate and is designed to identify what projects, activities and initiatives organisation responsible for ICT implementation in Malawi is intending to undertake in the coming year. Each planned activity should be aligned to an ICT Goal expressed in the ICT Division Plan.

For each ICT Goal, the Division identifies:

- the planned activity or objective that to be activated,
- identify the overall project manager,
- identify any budget and resources,
- identify the key milestones and/or outcomes,
- Identify the timeframe (Start and End Dates),
- Identify the person responsible for achieving the milestone.

A Risk Assessment (mandatory) will accompany each planned activity or objective and will:

- describe the risk,
- suggest possible causes,
- suggest the likelihood of the risk occurring, suggest the consequences should the risk occur, attribute a risk rating.

ICT Capital Investment Plan (3 year timeframe)

The ICT Capital Investment Plan identifies major planned Government/Organization Projects that have a significant ICT Capital component over a rolling three year timeframe, based on input from the Organizational Strategic Plans, communicated to the CIO and the ICT Steering Committee. This plan also identifies the non-capital components to provide a total estimated expenditure. This Plan is approved by the ICT Steering Committee.

ICT ORMP (1 year timeframe)

Senior Managers should compile a yearly ICT Organizational Resource Management Plan (ICT ORMP), detailing their expected needs for the coming year related to ICT, their proposed ICT projects, and an up-to-date information security risk management profile for the organization.

The ICT ORMP also requires Organizational Senior Managers to compose a functional assessment of employee position against designated equipment (Function vs. Equipment Assessment). The assessment describes the functions of each employee position and the ICT requirement to support said function. Depending on the degree of

work, ICT equipment such as personal computer systems and laptops may be designated to a specific employee position or for common use of a specific function.

Within the Government Finance environment, Organisation responsible for ICT implementation or regulation in Malawi ICT staff embedded in Ministries/Departments is allocated to a specific project code. The ICT ORMP apportions the salary and non-salary costs against each ICT project.

ICT Meeting Schedule

The ICT Unit should convene a tiered system of Meetings that address strategic, tactical and operational matters. The structure should be as follows:

- ICT Executive Management Team
- ICT Managers Meeting
- Organizational Managers and ICT Unit Managers Meetings (meets scheduled as required).

3.10.2.3 ICT Review

The ICT Unit, on behalf of the CIO, maintains and refers to a number of information sources to assist and inform the planning process. These include:

Financial

- Each month, for each Project, an ICT Financial Project Report should be run to ensure that project expenditure is within budget limits as determined by the ORMP allocation.
- Each Quarter, the Unit is required to submit a Quarterly Budget Review and identify any extraordinary items that are likely to result in the Unit exceeding the ORMP budget allocation.
- ICT Recurrent budget expenditure.
- ICT Workforce Profile reports and Termination and Absence reports (updated quarterly).

Operational

- Prior to each meeting of the ICT Steering Committee, the CIO provides a comprehensive report detailing activities since the previous meeting. The summarized performance and trends including: GWAN availability and level of utilization, Internet traffic, e-mail and spam traffic, staff surveys, SLAs, and ICT compliance activities.
- Resource allocation by section and team.
- Network and Server utilisation monitoring.
- Audit and Risk Committee reports on progress towards achieving Audit Findings.
- Relationship Management reports and Service Level Agreement reports.

3.10.2.4 ICT Value Decision-Making

The ICT Steering Committee is regularly confronted with a diverse range of potential proposals to consider. Deciding which ones to proceed with can be a vexing issue. To assist members of the ICT Steering Committee make decisions that are more likely to result in Value being realised, GOM/Organization should utilise the resources and templates provided by ISACA under the Val IT governance framework.

Val IT supports the business goal of realising optimal value from IT-enabled business investments at an affordable cost with an acceptable level of risk. The Val IT principles are:

- IT-enabled investments will be managed as a portfolio of investments.
- IT-enabled investments will include the full scope of activities that are required to achieve business value.
- IT-enabled investments will be managed through their full economic life cycle.
- Value delivery practices will recognise that there are different categories of investments that will be evaluated and managed differently.
- Value delivery practices will define and monitor key metrics and will respond quickly to any changes or deviations.
- Value delivery practices engage all stakeholders and assign appropriate accountability for the delivery of capabilities and the realisation of business benefits.
- Value delivery practices will be continually monitored, evaluated and improved.

Organisation responsible for ICT implementation or regulation in Malawi has adapted and developed the Val IT Project Rating Tool for use by the Organization Analysts to assess and rate the viability and value delivery of various project proposals. Members of the ICT Steering Committee will utilise the same Project Rating Tool to rate these same proposals.

The Government of Malawi Project Rating Tool appears on the following page.

3.10.3. Government of Malawi - ICT Project Rating Tool

Cells on this row are worth	Directive	Business **Impact**	**Benefits Realisation**	**Customer Service**	**Business Analyst Assessment**
1	Approved by ICT Steering Committee as contributing to the Government's Strategic Goals	Essential to sustain business operations.	This is a key element of the GOM strategic plan. Major improvements expected in business process.	This will deliver major service improvements for all customers.	**Outcomes**
0.9	Approved by CIO	As above.	This is a key element of the Ministry or Department strategic plan. Benefits >> cost	This will deliver major service improvements for a specific customers group.	**Alignment**
0.8	Approved by Director	As above.	This aligns with the Ministry or Department strategic plan. Benefits >> cost	This will deliver some service improvements for all customers.	**Financial benefits**
0.7	Ministry or Department Executive initiative	This will have a significant effect on longer term business operations.	This aligns with objectives of the section's business plan. Benefits > cost	This will deliver some service improvements for a specific customers group.	**Non financial benefits**

0.6	Ministry or Department Section initiative	As above.	This aligns with the section's operation plan. Benefits > cost	This will deliver minor service improvements for some customers.	**Resources**
0.5	Resulting benefits are not very clear.	This will have a significant effect on short term business operations.	There is little connection to any strategic plan. Cost is greater than benefits	This will have little impact on customer service.	**Expenditure**
0.4	Unlikely to get funding support	As above.	This does not align with the section's operation plan. Cost is greater than benefits	This could deliver minor service degradation to some customers.	**Risk drivers**
0.3	There is no general consensus	As above.	This does not align with objectives of the section's business plan. Cost is much greater than benefits	This could deliver minor service degradation to all customers.	**Assumptions and constraints**
0.2	There is no directive from senior management to make this happen.	This will have a minor impact on business operations.	This does not align with the Ministry or Department strategic plan. Cost and benefit cannot be defined	This is likely to degrade service to some customers.	
0.1	There is no	As above.	This is contrary to the	This is likely to	

	identified business requirement to do this.		Ministry or Department strategic plan. There is no requirement to do this.	degrade service to all customers.	
0.0	Staff member initiative only	This will have very little impact on business operations.	This is contrary to the GOM strategic plan. There is no requirement to do this.	This will degrade service to all customers.	**BA TOTAL**
Score					**ICT Steering Committee TOTAL**

3.11. Tele-centres Management

3.11.1. Preamble

Tele-centres in Malawi have been constructed and established as a means for providing access to ICTs and library material (in some cases). Each tele-centre is run as a stand-alone facility with no common vision with other tele-centres or tele-centre projects. The tele-centres have been established by copying from other countries, with no regard to the local environment of the beneficiary communities. Neither the Central Government nor the Local Government has provided policy guidance or clear vision as to how tele-centres should be turned into knowledge hubs. Training on use of ICTs for local communities has not been given priority. The tele-centres, therefore, have been erected in the communities where the target group is ICT illiterate and/or there is no relevant information to empower the communities and transform their economies.

It is imperative, therefore, that Malawi should develop a model for tele-centres in order to guide future projects and transform those already operational from being ICT-focused into service-focused centres.

In recommending a model for the Malawian e-Community Centre model, it is important to critically consider the aspirations of the community that will be utilizing the centres. Primary among many questions from the local people, whose high percentages are women and the youth, is "How can I make more money?" and "How can I compete better with other youth/disadvantaged groups in privileged communities?" These two questions should help in shaping the model for the Malawian e-Community Centre.

3.11.2. Issues

In making recommendations for the Malawian set-up, the following issues have been considered:

a) Housing for the "Tele-centre"

For Government-driven initiatives, free housing for the facility has been provided. The Centre can be housed in a Government building or a purpose-built building. Problems associated with such arrangements include sustainability due to public institutions funding and management problems. The best scenario, however, should be where the building belongs to an entrepreneur.

b) Access equipment used at the centre should include:

- Computers for accessing and using Internet, emails, social networks and computer games;

- Printers for making hard copies;
- Fax for sending and receiving hard copies;
- Television for accessing broadcasted information and for entertainment;
- Telephone kiosk which could be located within the premises but accessible even after the centre is closed, provided that there is enough security against theft; and
- Tables and chairs can be used for discussions or for reading away from the computers.

c) Location of the "Tele-centre":

Site selection is very important. Ideally, the tele-centre should be within walking distance of very busy places or dwelling places. While remote communities are the primary focus, peri-urban and urban centres also need to be included in the master plan that should be developed by Government.

d) Content that the local people will find or have access to at the centre:

Where tele-centres have flourished, the staff in that centre have researched and searched for content that would be relevant to the local community, made a catalogue that the local people would refer to as they utilized the centre. Combining the tele-centre with library facilities has also proved very beneficial.

Government, with the intention of promoting access to Government services by the citizens and the general public, could ensure that information such as the following is accessible electronically through the centres:

- Government forms (passports, licenses, etc) and submission of applications for services;
- Government announcements;
- Information on Government's programmes;
- Parliamentary proceedings;
- Awareness on Malawi Laws & Regulations;
- Status on court proceedings;
- Access to domestic and international markets that are relevant to the community's economic activities;
- Access to domestic and international learning material;
- e-Learning for Primary schools/e-literacy;

- Access to medical and health information;
- Access to medical care givers;
- Access to agricultural information;
- Access to results of research done in various sectors; etc.

It is important to remember that the local people have traditionally gone to the Government to seek assistance and services. In reality, though, "Government" is divided into specific Ministries, with each Ministry producing unique products, services and information. Government should, therefore, ensure that the "tele-centre" and the online information follow the same perception of the local citizen of "one Government" or "one-stop shop". The information, therefore, should be citizen-centred as well as service-oriented and not Ministry or sector specific. Government needs to package information for easy access by the local citizen.

Without relevant content being found at the tele-centre, the structures will remain white elephants.

e) Affordability for the local citizen

Citizens in the local communities are generally hard-pressed for financial resources. As Government ensures that "tele-centres" are sprouting all over the country with content that would empower and facilitate active participation of the local citizens, access to the information by individuals could be hampered by the gap between the cost of access and the economic levels of the citizens. Government, therefore, needs to put in place mechanisms for subsidizing the cost of Internet for tele-centres that are located in rural and peri-urban centres.

f) Training

The tele-centres must have space for training the local people on how to use ICTs. This will have an impact on how the citizen readily takes up ICT as a tool for their personal improvement and the development of the community. This is in recognition of the fact that ICT literacy is very low in the country and the local citizens will be afraid to use technology in the absence of proper hand-holding.

Young people should be encouraged to form Internet clubs that would hold meetings to encourage, train and support each other as they discover the power of the Internet.

g) Publicity and Sensitization

As Government intensifies the provision of information through "tele-centres", the general public needs to be sensitized on the facilities available and

information that can be accessed from the "tele-centres". Sensitization messages should be built into activities done by existing institutions such as the Ministry of Information, Ministry of Education, and the NICE, just to mention a few. More publicity can be built into e-Government publicity activities within the Mass ICT Literacy programme. NGOs can play an active role in sensitizing the general public on the power of the "centres".

h) Networking for the "tele-centres"

A tele-centre is a last mile connection. Some tele-centres will be connected directly to a main backbone while others are part of a 'last-mile' connection.

Regardless of how geographically for a tele-centre is from a main backbone, the local area network in the tele-centre should be as cost effective as it is technologically possible.

3.11.3. Business Model

A Public-Private-Partnership arrangement for managing the "tele-centre" initiative. For instance, government could encourage private to invest in a tele-centre by delivering e-government services through the tele-centre at a fee. Public-Private-Partnerships will offer financial sustainability and sustainable utilisation of the tele-centre.

3.11.4. Roles and responsibilities

3.11.3.1 Role of Government in the Tele-centres

Government through the department for e-government services will promote implementation of tele-centres and through the Malawi Communications Regulatory Authority will regulate the tele-centres.

3.11.3.2 Role of the Business Community in Tele-centres

The Private Sector and the business community's role is to make investments in establishing and managing tele-centres as business ventures. They too can also provide content in line with the laws of Malawi.

3.11.3.3 Role of NGO's in Tele-centres

Non-Governmental Organisations can invest in tele-centres and they too can also provide content in line with the laws of Malawi.