

## Table of Contents

Foreword.....	3
List of Acronym .....	4
Glossary.....	5
Introduction .....	6
Compliance.....	6
Enforcement.....	6
ICT will be used to improve service delivery within government and key stakeholders. ...	7
Use of ICT is to be authorised.....	7
Data is to be managed in such a way as to ensure its integrity and security.....	8
Procurement of ICT services and products is to be conducted in line with government tender and buying procedures.....	9
The Management of Projects should include monitoring of key project tasks and risk management principles. ....	11
Assurance of the Security of systems and network infrastructure is required. ....	12
<i>Physical Security</i> .....	12
<i>Virus Management</i> .....	12
<i>Internet and e-mail security</i> .....	12
<i>Security of IT Equipment assigned to users</i> .....	13
<i>Security using passwords</i> .....	14
<i>Authorisation Management</i> .....	14
Software applications are to be proactively managed and a maintenance programme is to be implemented.....	15
All DISTMS staff are to be trained to provide support and maintenance of the ICT.....	15
DISTMS are to adhere to all IT Procedures. ....	16

## Foreword

Information and Communications Technology (ICT) is one of the fundamental socio-economic development tools. It is not uncommon to hear a person say "Information is powerful". Whether the person says that cautiously or uncautiously, it is obvious that without information there is ignorance. But for the information to be powerful it must be timely and accurately communicated. The technology with which information is handled will therefore affect the power of the information.

The Government of the Republic of Malawi has made specific policy initiatives that recognise the role of information and communication technology in socio-economic development of Malawi. In 1998 Government passed a Communications Act that focuses on broadcasting and media. In mid year 2002, Government appointed a Malawi National ICT committee to develop a Malawi National ICT Policy and corresponding legislation. Recently, efforts to develop Malawi Civil Service ICT policy and corresponding standards were initiated and finalised. This policy document is a result of the recent initiatives.

This ICT policy document provides methodologies and standards with which to promote proper development and utilisation of ICT in the Civil Service. I expect that all ministries and department will join my office's commitment to implement this Malawi Civil Service ICT policy.

I would like to thank the World Bank for providing FIMTAP preparation financial resources which enabled the development of this policy. I would also like to thank Ernst and Young for technical expertise in the development of this policy. Further appreciation goes to the Principal Secretaries and their officers who participated in the development of this policy and to the Department of Information Systems and Technology Management Services for conducting the development process.

**A.A. UPINDI**

**Secretary to the Office of the President and Cabinet**

## **LIST OF ACRONYMS**

Backup	A copy of a file
CGIS	Central Government Information System
DISTMS	Department of Information Systems and Technology Management Services
FIMTAP	Financial Management, Transparency & Accountability Project
GoM	Government of Malawi
GWAN	Government Wide Area Network
Housekeeping	Orderly management and storage of files on a PC
ICT	Information and Communications Technologies
IFMIS IT	Integrated Financial Management Information Systems Information Technology
KPI	Key Performance Indicators
LAN	Local Area Network
LGIS	Local Government Information Systems
OPC	Office of the President and Cabinet
PC	Personal Computer
PPPAI	Payroll, Pensions and Personnel & Advances Integrated System
WAN	Wide Area Network

## **GLOSSARY**

Computer systems	A combination of computer hardware, software and peripherals.
Confidential data	Data whose access should be restricted by nature of its contents.
DISTMS	Is a department responsible for the promotion of ICT development and utilisation in the Civil Service
ICT	Is the technology with which information is captured, processed, stored and distributed.
Invaluable data	Not valuable data.
IT	Is ICT without the 'C'. Very often IT and ICT are used interchangeable. Equating of IT to ICT has been made possible by the convergence of Information Technology (the technology with which information is captured, processed, stored, retrieved and distributed) and communication technology (the technology with which information is disseminated, relayed or distributed).
Owner of Data	Is the Principal Secretary of a Ministry or the head of a department, whichever is applicable, to which the data belongs.
Senior Gov. staff or Servant	The Civil Service officer authorised to commit his/her Senior Civil office to expenditure.
User of data	Is a Civil Servant or such officer authorised by owner of data to use the data.
Valuable data	Data whose value may not erode with time. Such data includes but not limited to financial or contractual records.

## **Introduction**

The document presents the Malawi Civil Service ICT Policy. This policy has been developed to ensure uniform development and utilisation of ICT across the Civil Service.

The Malawi Civil Service ICT Policy forms part of the Terms and Conditions for Employment of all Civil Service staff. In addition, staff on secondment to Government of Malawi and all external Contractors should adhere to the same policies.

This document is to be read in conjunction with ICT Guidelines and the new Information Systems Security Policy.

## **Compliance**

Compliance with these policies and procedures is mandatory.

Staff are required to sign an annual compliance declaration, which includes IT security and compliance with procedures.

Contractors and others are required to sign a declaration at the commencement of their provision of services to the Government of Malawi, stating that they have read and understood these statements and will comply with them.

□The DISTMS shall ensure that the Civil Service ICT Policy, Strategic plan and related standards is considered when developing and reviewing the Malawi National ICT policy and study or any other related policy such as Malawi National Science and Technology policy.

## **Enforcement**

Responsibility for enforcement of this policy lies with each Ministry and Department within the Government of Malawi. Ministries, Departments and DISTMS share the responsibility of implementing this policy. DISTMS will act with Department of Human Resources to ensure that any instance of deliberate noncompliance by a staff member is:

- Treated seriously; and
- Addressed in line with the Disciplinary Procedures set out in the Staff Manual, The Malawi Public Sector Regulations (MPSR) document.

### **1. ICT will be used to improve service delivery within government and key stakeholders.**

- 1.1 Information will be made available in an appropriate format to all authorised stakeholders.
- 1.2 Awareness of ICT to be promoted within the public sector and key stakeholders.
- 1.3 Each member of Government Ministries and Department is responsible for managing information and managers are accountable for the ICT component of outcomes.
- 1.4 Accessibility of data to stakeholders must be documented, approved and made available as per the documentation.
- 1.5 Data is to be stored and retrieved in an authorised format.

## **2. Use of ICT is to be authorised.**

- 2.1 Use of ICT should be restricted for the furtherance of the Government's business and development of the ICT infrastructure and should not be for personal benefit.
- 2.2 Investment of ICT must contribute towards achieving Government strategic goals.
- 2.3 ICT services and facilities may not be used for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by the Government of Malawi.
- 2.4 The access, downloading or distribution any material, or issuance of statements, opinions or comments via the governments systems, which are pornographic, racist, sexist or otherwise discriminatory, illegal, or likely to cause offence are not allowed.
- 2.5 Access to ICT other than through the appropriate, authorised channels is not permitted. Offenders will be disciplined through the appropriate channels.

## **3. Data is to be managed in such as way as to ensure its integrity, security and resilience.**

- 3.1 Each data set shall have an owner, referred here in as 'Owner of data', and shall have users referred here as 'Users of data'
- 3.2 Owners of data shall determine users of data, which set of data each user of data is permitted to use, and the type of transaction the user of data is permitted to operate on the data.
- 3.3 ICT must be managed holistically to ensure integration of Government systems and resources.
- 3.4 Data must be stored and managed centrally.
- 3.5 Access to Data must be secure.
- 3.6 Each Government Department must consider and include ICT in their strategic objectives and plans. These must be updated annually in line with strategic objectives.
- 3.7 Access to information to the public and stakeholders should be given in the required format and to authorised personnel.
- 3.8 Make appropriate database backups and archives for each system (usually daily) and where client server facility is available, data must be transferred to the server via LAN.
- 3.9 Invaluable data stored on disks and other storage mediums is to be destroyed once it is no longer required.
- 3.10 Valuable data stored on disks and other storage mediums should be stored in fire and water proof lockable cabinets. When the data is no longer required the owner of data should request Malawi National Archives to archive the data. No unauthorised personnel are allowed to use your ICT equipment.
- 3.11 All floppy disks and other data storage media are to be secured when personnel are away from their work area.
- 3.12 No additional copies of confidential data without the permission of Senior Managers and government are to be allowed.

**4. Procurement of ICT services and products is to be conducted in line with government tender and buying procedures.**

- 4.1 Adopt standard Government tender procedures and requirements for procurement and employ the standard tender and procurement procedures. The Government of Malawi has already adopted World Bank ICT procurement guidelines.
- 4.2 Items to be purchased are to be standard ICT products that are reliable, flexible and adaptable to the Malawian environment, and have built in best practice and standards.
- 4.3 A feasibility study is a prerequisite to the procurement for all ICT products and services other than consumables.
- 4.4 A detailed specification of product and service requirements must be documented agreed and formally signed off by senior Government and IT staff prior to commencement of procurement process.
- 4.5 Tender documents for procurement of ICT products and services must be compiled and circulated in accordance with Government tender procedures and regulations.
- 4.6 Tender process and documentation are to be communicated to bidders.
- 4.7 An evaluation criteria based on the requirements specification must be defined and documented prior to receipt of tender bids.
- 4.8 Bids are to be received and opened in accordance with Government tender procedures and regulations.
- 4.9 Bids are to be evaluated according to the predefined evaluation criteria. All scoring and evaluation results of bids must be documented.
- 4.10 Systems are to be selected on the basis of assured system continuity and local support.
- 4.11 In the event that bespoke systems are implemented, Government are to ensure that the supplier guarantees local maintenance and support as a condition in the contract.
- 4.12 The highest scoring bid should be selected.
- 4.13 Contracts should include payment conditions that are performance based.
- 4.14 Contracts are to be drawn and signed by the Government and the successful bidder prior to commencement of the project. Such contractor should use the Malawi Civil Service (ICT) standard contracts released by government as part of this policy.
- 4.15 In the event that contract negotiations are unsuccessful, the activities leading up to this point must be documented, and valid reason included for the breakdown in negotiations. Contract negotiations with the second highest bidder should follow.
- 4.16 Unsuccessful bidders are to be notified in writing.
- 4.17 The project scope, methodology and implementation plan must be agreed to at the outset of the project. These must be documented and signed off by Government, suppliers and third parties.
- 4.18 Payment to suppliers of products and services must be approved and performance-based.

- 4.19 All systems configuration and development documentation must be in possession by the Government prior to final payment.
- 4.20 Regular progress reporting and evaluation must be carried out at predefined intervals during the implementation process.
- 4.21 User Acceptance Testing and sign off of system performance and functionality must be obtained.
- 4.22 Support and maintenance agreements must be entered into prior to completion of projects. The Malawi Civil Service sample ICT standard contracts should be used.
- 4.23 Service Level Agreements must be drawn up and entered into with all third-party suppliers.
- 4.24 Internal Service Level Agreements between DISTMS and Government users for maintenance of existing ICT's are required.
- 4.25 All documents related to the procurement process shall be labelled "Valuable data".

**5. The Management of Projects should include monitoring of key project tasks and risk management principles.**

- 5.1 A Project Manager is to be appointed prior to the commencement of an ICT Project.
- 5.2 The Project Manager will be responsible for the following:
  - Defining the project scope;
  - Allocating budgets and resources;
  - Documentation of the system requirements
  - Managing project and system related risks;
  - Monitoring of project deadlines and commitments;
  - Instating and implementing controls and IT Policy measures for the project;
  - Maintaining all project documentation;
  - Communicating project objectives, issues and progress;
  - Arrangement of training for all users in system functionality;
  - Monitoring of the Project Budget; and
  - Facilitating the transfer of ownership of the system to the end-users.
- 5.3 All development performed during an IT Project must be documented and subscribe to government standards and procedures.
- 5.4 All project meetings must be recorded in the form of minutes and filed for record purposes.
- 5.5 All project decisions must be documented and filed for record purposes.
- 5.6 All project payments must be documented.
- 5.6 All documents related to the project decisions and payments shall be labelled "Valuable

data”

**6. Assurance of the Security of systems and network infrastructure is required.**

***Physical Security***

- 6.1 No unauthorised persons are to gain entry to Government premises without the permission of authorised Government staff.
- 6.2 All storage media such as floppy disks, magnetic tapes and CD ROMs containing government data must be physically secured when not in use.
- 6.3 Equipment may not be moved or relocated without the approval of ICT Committee.
- 6.4 ICT Equipment in high-risk areas is to be secured.

***Virus Management***

- 6.5 Data integrity checking software is to be upgraded as soon as the new release is available
- 6.6 All files received and sent out, including floppy disks, are to be scanned using virus detection software.
- 6.7 No attempts are to be made to prohibit the running the anti-virus scan in automatic mode.
- 6.8 Antivirus updates are to be updated on each PC at least once a month.
- 6.9 Confidential or personal information may not be given out over the phone.
- 6.10 Dial-in facility to any external software support staff and download software from electronic bulletin board systems, external electronic mail systems, external communication networks, the Internet, or other systems outside of the Governments ICT is prohibited. All requests should be made through the ICT Committee.
- 6.11 Where users suspect that their PC has been infected with a virus, they are to report this to DISTMS immediately.

***Internet and e-mail security***

- 6.12 DISTMS shall annually predefine the maximum size of a single e-mail. File size for each e-mail, including attachments, should not exceed the predefined maximum size.
- 6.13 Do not send or receive electronic mail or electronic data by any means other than those officially installed and supported by the DISTMS.
- 6.14 Do not automatically forward, or divert by any means, mail from your government mail account to any other non-government mail account.
- 6.15 Do not use e-mail externally where security is important.
- 6.16 Do not fax documents of a highly confidential nature unless appropriate security measures can be taken.
- 6.17 Do not allow the use of an Internet connection unless explicit approval is given.
- 6.18 Always use a firewall for Internet access

### ***Security of IT Equipment assigned to users***

- 6.19 Implement security measures to protect the government's ICT equipment and other property at all times, which includes compliance with planning, building, fire, flood, local government and DISTMS safety regulations.
- 6.20 Ensure that workstations and servers are outfitted with Uninterrupted Power Supply (UPS) systems, electrical power filters, or surge suppressers that have been approved by DISTMS.
- 6.21 Do not alter computer equipment configuration without the knowledge and authorisation of the Systems Administrator; this includes upgrading the processor, expanding the memory or adding extra circuit boards.
- 6.22 Do not smoke, eat or drink in the proximity of ICT equipment.
- 6.23 Do not connect unauthorised equipment to the LAN or WAN; all connections must be installed by DISTMS.
- 6.24 Do not connect dial-up modems to workstations that are connected to a LAN or WAN without the express permission from the DISTMS Systems Administrator.
- 6.25 Implement the prescribed 'Disaster Recovery Procedures' in the event of system failure.

### ***Security using passwords***

- 6.26 Use your DISTMS-approved screensaver together with a password when away from your PC.
- 6.27 Protect confidential documents created in Word or Excel by using a password to prevent alteration.
- 6.28 No passwords or ID\* are to be shared.
- 6.29 DISTMS may not disclose passwords via telephone lines or e-mails; passwords should only be communicated in person.
- 6.30 Passwords are to be kept secret\* and changed regularly.
- 6.31 Passwords that cannot be easily guessed must be used and passwords of a minimum of 6 characters in length are required.
- 6.32 No passwords may be stored in a readable form; this includes automatic login scripts, software macros, terminal function keys and other locations where unauthorised persons may discover them.

### ***\* Unless required for support purposes***

- 6.33 All passwords suspected of being disclosed, or known to be disclosed to unauthorised parties must be changed immediately.

### ***Authorisation Management***

- 6.34 Only create new users on the systems where the number of user licenses has not been exceeded.
- 6.35 The creation and Maintenance of users is the responsibility of the 'Authorisation

Manager' or a designated person within DISTMS.

- 6.36 Creating detailed job roles and responsibilities for all system users will be the function of DISTMS.
- 6.37 The Authorisation Manager will be responsible for the following, written approval from the relevant government department:
- Creating new users in the system
  - Changing user authorisations in the system
  - Deleting users and user authorisations in the system
  - Maintaining documentation for user authorisations
  - Installing controls that ensure recording of all logins, successful or unsuccessful

**7. Software applications are to be proactively managed and a maintenance programme is to be implemented.**

- 7.1 All software installations on government computer systems shall be done with the knowledge of the corresponding owner of the computer systems. All software installations on government wide computer systems shall be done with the knowledge of DISTMS
- 7.2 No copies of licensed software are to be made without the licencer's approval.
- 7.3 No government owned software is to be installed on personally owned PC's.
- 7.4 No system changes to government wide software or software on GWAN without authorisation from DISTMS are permitted.
- 7.5 An audit trail of system changes is to be maintained by DISTMS.
- 7.6 The installation, launch, download, save or sending of any computer games, wallpaper files, screen savers, bitmap files, video clips or any 'executable' files e.g. software or files with the following file name extensions – .exe, .com, .avi, .mpeg, .bat is not allowed. Where permission is granted to install such software, DISTMS should be responsible for installing the software.
- 7.6 The number of users licensed for all software are to be documented. \*
- 7.7 All software malfunctions are to be reported to the DISTMS help desk. The help desk staff are to document all failure and follow-up on reports to ensure the problem is isolated and resolved.

***\*Failure to do so may result in litigation from the software developers.***

**8. All DISTMS staff are to be trained to provide support and maintenance of the ICT.**

- 8.1 All government staff are to be equipped with appropriate ICT training for the job description.
- 8.2.1 Develop and retain knowledgeable staff to maintain and support the ICT as well as perform further development of the governments ICT.
- 8.3 Trained staff are to be retained within the government using the government's retention policy for IT personnel. In the event that staff have to leave the Civil Service, a formal handover and knowledge transfer process should be conducted.

- 8.4 Human Resource officers in DISTMS and the ministries shall source appropriate training courses for ICT staff.
- 8.5 A Human Resource management information system shall be used to keep a record of all training attended by the ICT staff.
- 8.6 Training, knowledge and skills transfer is to be an on-going process for DISTMS and government staff.

**9. DISTMS are to adhere to all IT Procedures.**

- 9.1 Procedures involving installation and upgrade of hardware, software, scripts and patches are to be maintained by DISTMS.
- 9.2 Procedures for disaster recovery are to be implemented in the event of system failure.
- 9.3 Back-up and storage schedules and procedures are to be maintained and implemented by DISTMS.
- 9.4 Procedures for user creation and deletion, user profiles creation and changes are to be maintained and implemented by DISTMS.
- 9.5 Procedures illustrating communication channels between the IT Department and the Business Units are to be maintained and implemented by DISTMS.
- 9.6 Procedures for problem escalation and resolution between the IT Department and the user community are to be maintained and implemented by DISTMS.
- 9.7 Procedures outlining physical security maintenance of the buildings, network, hardware and all other equipments are to be maintained and implemented by DISTMS.
- 9.8 Procedures demonstrating the conversion process of data, interfaces and the preservation of databases are to be maintained and implemented by DISTMS.
- 9.9 Procedures for dial-in facilities and access to ICT resources by third parties are to be maintained and implemented by DISTMS.