

TABLE OF CONTENTS

[Table of Contents](#) i

[Introduction](#) 1

[Purpose](#) 1

[Links to Other Documents](#) 1

[Background](#) 1

[Objectives](#) 2

[Structure of Security Documentation](#) 3

[Security Principles](#) 3

[Scope](#) 3

[Compliance](#) 4

[Incidents](#) 4

[Security Roles and Responsibilities](#) 5

[Security Organisation](#) 5

[Government Security Officer](#) 7

[Health & Safety Officer](#) 7

[Site Security Officers](#) 8

[Legal Advisor](#) 8

[Information Security Officer \(GWAN\)](#) 9

[System Security Officers](#) 9

[Core Security Management Principles](#) 10

[Classification Scheme, Information Labelling and handling](#) 10

[Confidentiality classification system](#) 10

[Acceptable Use](#) 12

[Compliance with Legislation Requirements](#) 12

[Security Administration and Access Control](#) 13

[Information Security Standards](#) 14

[Malicious Code](#) 14

[Remote Access](#) 15

[Mobile Computing](#) 15

[Internet Usage](#) 15

[Electronic Mail](#) 16

[Security Awareness](#) 17

[Secure Systems Design and Implementation](#) 17

[Network Interconnection](#) 17

[Security in Contracts](#) 18

[Personnel Security](#) 19

[Assurance Approach](#) 20

[Key performance Indicators](#) 20

[Routine Security Audits](#) 20

[IT Security Code of Practice](#) 21

[Protection of Property](#) 21

[Restrictions on Use](#) 21

[Authorised Software](#) 21

[Authorised Hardware](#) 22

[Access Control](#) 22



Information Systems Security Policy

Virus Controls	22
Back-Up	22
Protection of Removable Storage Media	23
Internet Use	23
Removal of IT Equipment	23
Guidance and Training	24
Disciplinary Action	24
Declaration	24
Internet Security Code of Practice	25
Acceptable Business Uses	25
Unacceptable Business Uses	26
Illegal and Unethical Uses	26
Anti-Virus Measures	27
Reporting of Security Breaches	27
Declaration	27
Logical Access Control	28
Authentication	28
Access Privileges	28
Access Administration	28
Housekeeping and Audit	29
Network Services	30
System and Network Connections	30
Routers & Hubs	30
Gateways	31
VPNs	32
Firewalls and Proxies	32
Internet Connections	34
Internet Sites	34
Dial-Out	35
Remote Access	35
Malicious Code	36
Encryption	36
FTP	37
Telnet	37
Software Licensing	37
Physical Security	38
Personnel Security	38
Security Monitoring	39
Security Assurance	39
Contingency Arrangements	39
Maintenance	40
Virus Procedures	41
Appendices	43
Information Security Terms	43
List of Abbreviations Used	46



INTRODUCTION

Purpose

The purpose of this document is to formally outline the security policy for the Government of Malawi. This document is based upon information gathered from various stakeholders within the Government together with our current state assessment of the risks to the security of the Government's information and data.

These policies will require formal validation and approval by the Government of Malawi prior to implementation. Implementation processes are not set out within this document.

Links to Other Documents

This document should be read in conjunction with:

1. Ernst & Young's technical tender application in response to the Government of Malawi's Request for Proposal dated 28 June 2002 for Improving Management Systems and Information Flows.
2. Management of Computerised Systems – ICT Guidelines published by DISTMS
3. Ernst & Young's Current State Security Assessment of GWAN.
4. Ernst & Young's ICT Requirements Analysis for the Government of Malawi.
5. Ernst & Young's ICT Policy and Strategy for the Government of Malawi.

Background

The Financial Management, Transparency and Accountability Project (FIMTAP) is being undertaken by the Government of Malawi to promote effective and accountable use of public expenditures by improving the public sector management capacity and promoting effective and accountable use of public expenditures through improved budget implementation and increased transparency of Malawi Government institutions.

This deliverable is part of a wider consultancy designed to provide services in three areas relating to Improving Management Systems and Information Flows, namely:

1. Wide Area Computer Network design;
2. Electronic Information Security and Facilities Management; and
3. Civil Service ICT policy and strategy development.

This Information Systems Security Policy document is the second deliverable pertaining to the Electronic Information Security and Facilities Management engagement.



Objectives

The objectives of the information security policy are to:

1. Provide an appropriate level of security support such that the facility resources are protected from significant disruption;
2. Appropriately protect information stored on the facility computers from modification and disclosure;
3. Incorporate security measures from the start of a project's development;
4. Facilitate the timely identification and reporting of security incidents and breaches;
5. Provide a mechanism for the facility to recover from disruption so that the facility and clients are not adversely affected by computer security measures.

This document is designed to set out the information security policies for the Government of Malawi and to serve as a guide to the level of security that will be implemented.



STRUCTURE OF SECURITY DOCUMENTATION

Security Principles

Information security management is designed to address all information assets required to support Government processes. This includes paper records, voice communications and all forms of electronic data. Information security implies the need for:

1. **Confidentiality** - Information must only be revealed to those with authority to see or hear it.
2. **Integrity** - Information must be created, processed and communicated only by, and in the form intended by, those with authority to do so. That is, information must not be inserted, modified, deleted, mis-directed, replayed or otherwise abused.
3. **Availability** - Information, and the services required to access, process and communicate information, must continue to be available at the times agreed with users.

Accurate and timely information must be available to authorised users when and where required.

Scope

The scope of this document extends to all current and future systems used by the Government of Malawi to conduct its business.



All standalone PC applications are subject to the minimum security requirements contained within this document regarding PC security. However, due to the sensitivity of the data held on these PC's, Government should consider the implementation of additional physical (e.g. asset locks) or logical access security controls (e.g. BIOS passwords) to protect both the physical assets and the associated data.

Compliance

Everyone within the Government of Malawi, and those acting on behalf of the Government of Malawi, are responsible for the security of the Government of Malawi information assets entrusted to them.

Government of Malawi staff are not to disclose sensitive proprietary, contractual, supplier or staff related information to third parties, including friends and relatives, who do not have a need to know the information in order to meet their professional responsibilities to the Government of Malawi. Any approaches made by third parties to gain unauthorised access to sensitive the Government of Malawi information must be treated as a security incident and, as such, reported to an appropriate security officer. Access to computer systems, communications services and electronically held information is to be strictly limited to those staff who have an authorised requirement for such access.

Government of Malawi staff who do not comply with the defined security policies and procedures, or who knowingly or negligently allow staff under their supervision to do so, may be liable to disciplinary action, including dismissal.

Incidents

Any occurrence that detrimentally affects the security of the Government of Malawi assets and non-compliance with legal or regulatory obligations constitutes a security incident.

It is the duty of all Government of Malawi staff, whether permanent, temporary or contractor, to report to an appropriate manager any actual, suspected or potential breaches of security. All such incidents must be reported to the appropriate Security Officer.

Information security incidents should be investigated by the Government Security Officer or his subordinate, and appropriate action taken.



SECURITY ROLES AND RESPONSIBILITIES

The administration of the IT environment and infrastructure at the Government of Malawi is split between DISTMS and operations staff at each Ministry. Cognisance must be given to the proposed Data Centre, which may have an impact upon the roles and responsibilities defined in this document.

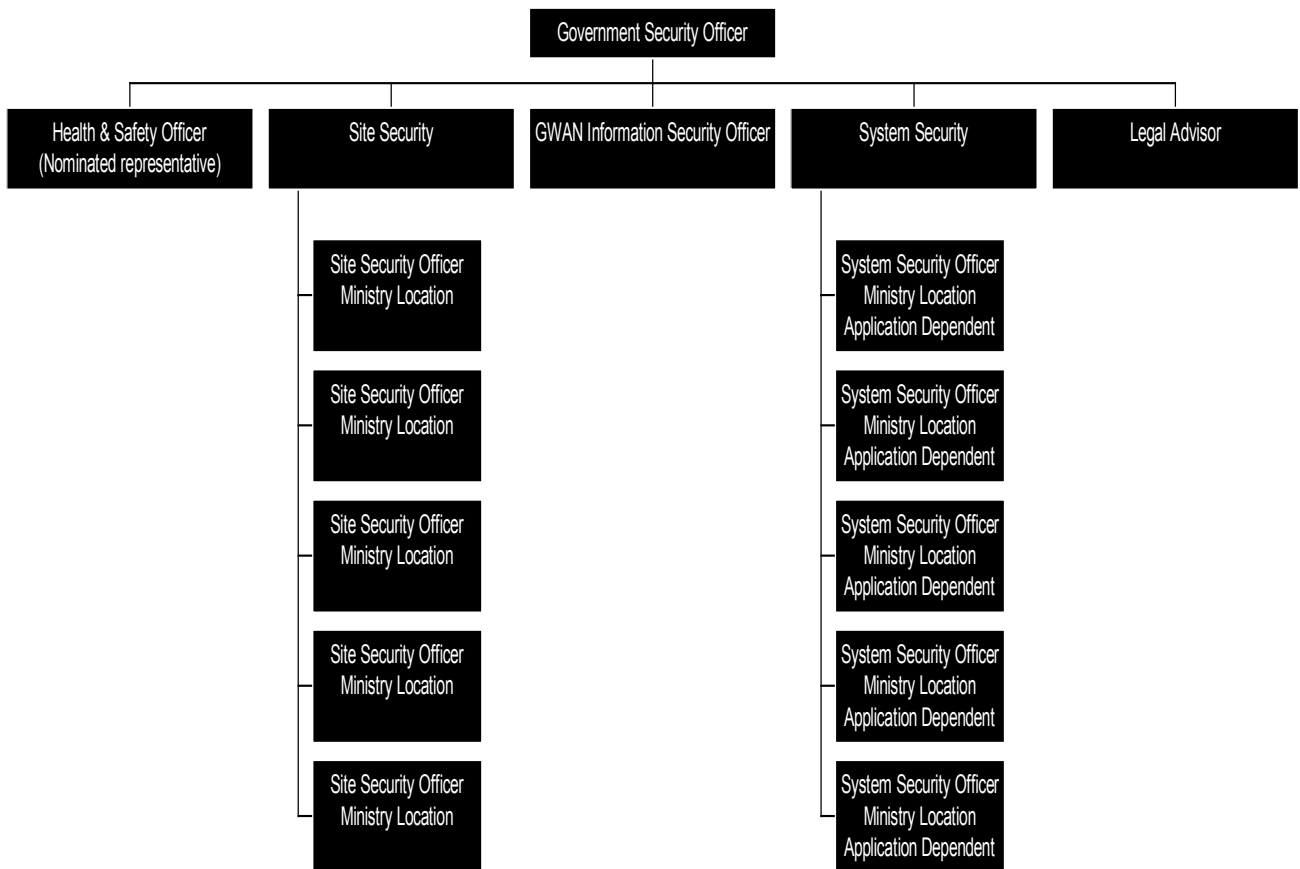
Due to the existing size of the IT infrastructure within the Government of Malawi and the limited usage of IT within the Government, multiple roles defined below may be assigned to a single individual with an appropriate split of responsibilities to ensure that there is adequate segregation of duties in key areas.

Security Organisation

The following security organisation is proposed:



Information Systems Security Policy



Government Security Officer

The Government Security Officer will have overall responsibility for information security within the operations of the Government of Malawi. He will ensure that security is applied consistently across the operations of the Government of Malawi and ensure compliance with the Government of Malawi group policies and procedures.

Due to the existing size of the IT infrastructure within the Government of Malawi and the limited usage of IT within the Government, we believe that the role of Government Security Officer will only require a part-time commitment. This role will therefore form part of the responsibilities of an existing full-time member of staff. However, this needs to be reviewed periodically in line with the growth of the Government of Malawi's usage of technology and to determine whether there is not an incompatible segregation of duties.

Health & Safety Officer

The role of the Health and Safety Officer is to ensure that individuals work within a safe working environment, which promotes good health. He is included within this organisational structure as physical aspects of building and site design impact upon his responsibilities.

Due to the existing size of the IT infrastructure within the Government of Malawi and the limited usage of IT within the Government, we believe that the role of Health and Safety Officer will only require a part-time commitment. This role will therefore form part of the responsibilities of an existing full-time member of staff. However, this needs to be reviewed periodically in line with the growth of the Government of Malawi's usage of technology.



Site Security Officers

The Site Security Officer is responsible for the physical security of the Government of Malawi offices. He is responsible for guards, receptionists and the procedures and policies that they follow, where such measures are deemed to be appropriate.

This person(s) will assume responsibility for the physical security of their building, computer room and for all personnel performing physical security-related duties.

Due to the existing size of the IT infrastructure within the Government of Malawi and the limited usage of IT within the Government, we believe that this role will only require a part-time commitment. This role will therefore form part of the responsibilities of an existing full-time member of staff. However, this needs to be reviewed periodically in line with the growth of the Government of Malawi's usage of technology and to determine whether there is not incompatible segregation of duties.

Legal Advisor

The Legal Advisor is responsible for:

1. Advising upon security aspects of contracts; and
2. Notifying the Government Security Officer of the introduction of legislation or regulatory requirements that would require the updating of the Information Security Policy.

Due to the existing size of the IT infrastructure within the Government of Malawi and the limited usage of IT within the Government, we believe that this role will only require a part-time commitment. This role will therefore form part of the responsibilities of an existing full-time member of staff. However, this needs to be reviewed periodically in line with the growth of the Government of Malawi's usage of technology and to determine whether there is not incompatible segregation of duties.



Information Security Officer (GWAN)

The Information Security Officer is responsible for:

1. Maintaining this Information Security Framework;
2. Developing supporting procedures and standards for the Government LAN and WAN environment; and
3. Implementing appropriate security controls for the GWAN environment.

System Security Officers

The System Security Officer is responsible for the day-to-day management of security upon a given system, in accordance with this Security Policy. They are responsible for general administration activities, which may include some security elements (e.g. taking backups).

Due to the existing size of the IT infrastructure within the Government of Malawi and the limited usage of IT within the Government, we believe that this role will only require a part-time commitment. This role will therefore form part of the responsibilities of an existing full-time member of staff. However, this needs to be reviewed periodically in line with the growth of the Government of Malawi's usage of technology and to determine whether there is not incompatible segregation of duties.



CORE SECURITY MANAGEMENT PRINCIPLES

Classification Scheme, Information Labelling and handling

Security classification systems are used to categorise an organisation's information assets, according to their sensitivity, and to facilitate the appropriate and cost-effective allocation of protective measures. All identified information assets are classified as having one of several defined levels of sensitivity, and, thereafter, all assets of a particular classification are originated, stored, disseminated and destroyed to the same secure standard. Classification systems are designed to enable the Government to clearly articulate and readily appreciate the sensitivity of a project, system or item of information.

Confidentiality classification system

A confidentiality classification and marking system should be applicable to all Government of Malawi's information assets to ensure that it appropriately protects both its own information and that entrusted to it by others.

It would be unjustifiably expensive to protect all information assets to an equally high level; moreover, such action would result in relatively low value information being over-protected and the protective measures for highly sensitive information being discredited. Equally, protecting all information to a single medium or low level would result in some assets being under-protected and under-valued.

Security classification systems are used to categorise an organisation's information assets, according to their sensitivity, and to facilitate the appropriate and cost-effective allocation of protective measures. All identified information assets are classified as having one of several defined levels of sensitivity, and, thereafter, all assets of a particular classification are originated, stored, disseminated and destroyed to the same secure standard. Classification systems also enable the Government to clearly articulate and readily appreciate the sensitivity of a project, system or item of information.

The two components collectively form the security label for the information asset. The marking system will consist of two components: a hierarchical marking and a component marking.



Information Systems Security Policy

The hierarchical components are defined as:

Hierarchical Marking	Impact Assessment Rating	Description
Public	Low	Public domain information. Disclosures, modifications, or loss would cause no Government losses ¹
Internal Use Only	Medium	Disclosures, modifications, or loss would cause some Government losses
Confidential	High	Disclosures, modifications, or loss would cause significant material Government losses

The following compartment markings are defined:

1. The Government Wide Area Network
2. The IFMIS Application and any feeder systems
3. The DPD Financial Management system and any feeder systems
4. The PPPAI Application
5. Internal file and email servers
6. Standalone PC applications

The following principles are proposed for information labelling and handling:

1. Sensitive hard copy output should be labelled with the appropriate information label
2. The classification of sensitive magnetic media should be clearly marked
3. Individuals must not disclose sensitive or protectively-marked information, whether electronic or paper, to anyone within Government of Malawi that does not have a legitimate need to know the information in the normal course of their duties
4. Individuals must not disclose sensitive or protectively marked information, whether electronic or paper, to anyone outside of Government of Malawi, unless authorised through the proper mechanisms and in accordance with the relevant security policy

¹ **Losses** are defined as all consequential costs, included predicted lost revenue, lost investment and likely litigation and compensation costs, but excluding any indirect costs arising from lost reputation.



5. Sensitive hard copy and magnetic media should be disposed of in a secure manner
6. Information marked Confidential should not be transmitted via fax or other transmissions media.
7. Magnetic media and equipment containing such media should be labelled with the classification of the most sensitive information that is currently or has previously been stored on it
8. Individuals should only access Government sensitive information if they require it in the normal course of their duties
9. Government of Malawi will take action against individuals who access, or attempt to access, information in breach of the above policy, even if this information is not disclosed to another party. This may include disciplinary action or prosecution.

Acceptable Use

1. Government of Malawi computing facilities will only be used for legitimate Government of Malawi business purposes
2. Such facilities will only be used by Government of Malawi personnel or their agents who have signed a formal non disclosure agreement
3. Government of Malawi computing facilities may be used to meet personal training and development needs of Government of Malawi personnel providing this usage does not impact upon operational requirements.

Compliance with Legislation Requirements

The following legal requirements will be adhered to:

1. Software licensing requirements
2. Local data protection legislation
3. Local computer misuse legislation
4. Local laws on the use, exportation or importation of encryption technology
5. Local copyright and laws
6. The general requirements for financial accountability and other operating regulations

Government of Malawi will also seek to identify new legislation that may be required to be incorporated into this information security framework.

Government of Malawi will ensure that use of Government computing facilities does not infringe criminal or civil laws, such as laws regarding the storage or transmission of libellous, indecent or offensive material.



Security Administration and Access Control

1. Responsibilities for security management and administration as defined in this document will be clearly assigned to individuals
2. Training will be provided where appropriate
3. Systems will have a nominated System Security Officer
4. Systems will be protected by adequate physical measures that are commensurate with the security risks that apply
5. Users will be authorised by the System Security Officer using defined procedures
6. No request for access will be processed without the appropriate authorisations
7. An audit trail will be kept of all authorised instructions
8. A minimum standard of technical access control, authentication and security auditing mechanisms will be provided for all systems that are connected to the GWAN
9. All users will have individual user identifiers
10. All users will be required to authenticate themselves before access is granted to systems
11. Privileged access levels (e.g. system manager or security administrator) will require specific authorisations by the Government Security Officer
12. User access rights will be reviewed and confirmed with the System Security Officer every 12 months
13. A mechanism will be established for notifying the System Security Officer of new starters, leavers and transfers before they occur. A review will be performed at least monthly to ensure that redundant users are removed
14. There will be independent monitoring of the security of systems covering:
 - a. Changes to the user population;
 - b. Changes to access rights;
 - c. Access to sensitive information/resources;
 - d. Use of sensitive user-ids; and
 - e. Violation of passwords or access rights;



15. A procedure will be in place designed to ensure the reporting and escalation of security incidents
16. Each system will be assigned a maximum clearance of information that can be stored upon it.

Information Security Standards

1. Specific security standards will be developed for all platforms, taking into account availability of specific securing functionality
2. There will be a formal review and approval process for all security standards
3. A minimum standard will be defined for password management
4. There will be a standard naming convention for user, server and domain names
5. A minimum standard for system audit and account will be defined.

Malicious Code

1. All staff will be responsible for adhering to the malicious code policy, and will:
 - a. Ensure that virus detection software is regularly run as described in the anti-virus policy
 - b. Promptly report virus infections;
 - c. Virus check imported media (i.e. floppy disks, removable disks, tapes) before data is imported onto Government of Malawi systems
2. There will be a defined process for virus reporting and escalation
3. The GWAN Information Security Officer will monitor the effectiveness of anti-virus measures
4. Un signed ActiveX will not be permitted on any system
5. Java will be permitted, but the GWAN Information Security Officer will monitor the risk that it presents to the Government
6. Only properly licensed software from reputable sources will be loaded
7. All software will be virus checked before installation
8. No software (including patches, drivers and screensavers) will be downloaded from the Internet without the prior consent of the System Security Officer and the GWAN Information Security Officer



Remote Access

1. Remote access will only be allowed via facilities approved by the GWAN Information Security Officer
2. Remote access to systems will only be allowed if approved by the System Security Officer
3. A minimum standard will be defined for the strength of the authentication mechanisms used for remote access
4. Remote users and their access rights will be reviewed at least once every six months
5. The use of remote access facilities will be audited
6. Users will only be given remote access with the approval of their Principal Secretary
7. Restrictions on the location of remote access will apply

Mobile Computing

1. Procedures will be defined for the use of mobile computing facilities (i.e. laptops and portable computers)
2. Users of mobile computing facilities are responsible for safeguarding such equipment and should take all responsible precautions to prevent theft, loss or damage of such items. In particular users should:
 - a. Not leave equipment in unattended cars
 - b. Ensure that when staying in hotels, that the safety deposit boxes (if available) are used to store unattended equipment
 - c. And ensure that equipment is not left unattended at anytime
3. When presenting sensitive information to external audiences, the sensitivity of the information should be explicitly stated by the presenter at the beginning of the presentation, and sensitivity markings should be clearly visible
4. Information classified as *Confidential* or above should not be stored on mobile computing facilities. Should business reasons require such information be taken outside Government of Malawi premises, the information sponsor must grant approval

Internet Usage

1. All interaction with the Internet will be via centrally managed connections. Users should not connect Government of Malawi machines to the Internet themselves



Information Systems Security Policy

2. The System Security Officer will require authorisation from the appropriate Principal Secretary and Head of Section before internet or external email access is provided
3. Head of Sections will be held jointly responsible for any misuse of Internet facilities that staff who they approved may undertake
4. The Internet will only be used for legitimate Government purposes
5. Use of the Internet will be audited
6. Access to inappropriate web sites, such as those containing pornography, will be prevented
7. Users will not enter Government of Malawi into any form of contractual commitment via the Internet
8. Users will not publish information on the Internet outside of the content management process unless approval is obtained from their Principal Secretary and the System Security Officer

Electronic Mail

1. Users will not make statements within email that would be inappropriate to make upon paper. In particular, users will refrain from making libellous, inflammatory, or indecent statements that could result in the Government being liable to litigation or bring the Government of Malawi into disrepute
2. Users will not forward email to accounts outside of the Government
3. For all information classified at *Internal Use Only* or above, users will clearly mark all email with the information label
4. For all information classified at *Internal Use Only* or above, email will be encrypted if transmitted internally within the Government. Such information will not be sent externally by email without the prior approval of the information owner
5. Use of external Internet email servers, such as Hotmail.com is allowed, but will not be used for information classified as *Internal Use Only* or above
6. All emails transmitted to external destinations will include a disclaimer that states that any opinions made within the email are personal and may not be those of Government of Malawi
7. Users should comply with good internet etiquette when using email
8. Email should only be used for legitimate Government purposes
9. Users should not open or execute any attachments received via email, without first scanning for viruses or malicious code as specified by the policy for Malicious Software.



Security Awareness

1. The Information Security Policies will be distributed to all users of the systems within Government of Malawi
2. The Government will design an ongoing security awareness program to promote good security practices amongst the user population
3. The roles and responsibilities for management, delivery and monitoring of the security awareness program will be clearly defined
4. All users will be required to sign a declaration stating that they understand and agree to abide by the information security policies

Secure Systems Design and Implementation

1. Systems will be designed with security measures to protect the confidentiality, integrity and availability of Government of Malawi information
2. Security requirements will be clearly defined for system developments
3. Testing of security requirements will be performed prior to new systems entering service
4. A formal change management process will be established in order to assess the impact of any changes to existing systems

Network Interconnection

1. The GWAN Information Security Officer must approve connection of Government of Malawi networks to other networks
2. Clearly defined roles and responsibilities will be defined for:
 - a. Management of Government of Malawi own networks;
 - b. Management of networks connected to Government of Malawi, which are not owned by Government of Malawi; and
 - c. Management of the interface between Government of Malawi and other networks.
3. Service level agreements or memorandum of agreement will be defined with all organisations that connect to Government of Malawi. Such service level agreements will clearly identify any security requirements



4. Networks that are connected to Government of Malawi will have a documented security policy. An assessment of the suitability of this policy, and its compatibility with the information security policy of Government of Malawi should be performed prior to connection taking place
5. A formal security assessment of the impact of connection will be performed when connecting any new network to Government of Malawi's networks. Such an assessment should consider any additional threats that the connection may introduce to Government of Malawi, and if any new vulnerabilities are introduced
6. A change control process should be defined that allows the impact to Government of Malawi of potential changes to connected networks to be assessed and controlled
7. A change control process should be defined that allows the impact to connected network of changes to Government of Malawi networks to be assessed and controlled

Security in Contracts

The key principles for security in contracts should include:

1. A clear statement of the security requirements required by Government of Malawi;
2. Confidentiality agreements (at an inter-Government level) for contracts that involve Government of Malawi releasing Government sensitive information;
3. A statement that Government of Malawi has the right to audit the security controls implemented by the contractor
4. A statement that Government of Malawi reserves the right to review the security and control procedures and/or require a third-party review of such procedures
5. Statements that Government of Malawi assets in the care of the contractor be protected to the same level as required by the Government of Malawi Information Security Policy
6. Statements controlling partners releasing information to the press
7. Clauses that articulate the way that security is to be managed and refer to an appropriate service level agreement
8. A provision requiring that, if any changes in procedures which might impact on security are to be made, they are to be communicated to Government of Malawi within two working days
9. Mechanisms by which Government of Malawi is to be informed of any security breaches and other potentially significant security incidents



10. A key individual at Government of Malawi as the primary contact point on security management (not daily administration) issues, and a counterpart at the contractor for day-to-day liaison and
11. A senior member of the contractor's staff to whom serious issues may be escalated by Government of Malawi, and who is briefed with the commercial and security needs of Government of Malawi.
12. Confidentiality agreements within contracts of employment, and the contracts for contracted staff and
13. General indemnity clauses to cover computer misuse by partners or contractors.

These policy statements should allow flexibility for the legal department to deviate from them if necessary.

Personnel Security

1. A process will be defined that notifies system administrators of the departure or transfer of users, so that timely deletion of redundant users accounts can be performed
2. Disciplinary procedures will be defined for users who are found to be in gross breach of these security policies, or who are found to be engaged in computer misuse.



ASSURANCE APPROACH

Key performance Indicators

In order to allow the overall application of the Information Security Policy to be assessed on an on going basis, a number of security key performance indicators (KPIs), such as for system availability, will be produced.

The Government Security Officer will undertake a periodic review of performance against the specified and agreed security KPIs.

Routine Security Audits

Government of Malawi will undertake a periodic review of the effectiveness of security controls across the organisation.

The Government Security Officer is expected to define a programme of security reviews on an annual basis. These reviews may target any aspects of the security framework and may be undertaken by internal or external resources as appropriate.

In addition to programmed security reviews, a process will be implemented for the regular monitoring and inspection of major computer generated log files which may indicate the potential mis-use of Government of Malawi computing facilities.



IT SECURITY CODE OF PRACTICE

The policy outlined below applies to all Government of Malawi employees and contractors. It is designed to assist in both preserving the confidentiality, integrity and availability of the Government's information and IT systems and ensuring the correct and legal use of software. The detailed rules form part of the terms and conditions of employment.

Protection of Property

All Government of Malawi staff should take reasonable care of the Government's property, including computers, printers, communication links, recording media and other associated devices.

Restrictions on Use

Only authorised Government of Malawi staff are to operate or otherwise use the Government's IT systems. All such staff will be issued with unique User Identifications and passwords to access those systems that they are authorised to use; the use of those identifiers to access a System will be regarded as an undertaking to comply with both this Code of Practice and any other rules relating to the operation and use of the System concerned.

Members of staff are only to process Government information on IT systems (including communication links and recording media) that have been provided, and are either owned or leased, by Government of Malawi. Government information is not to be processed on any other IT systems.

Authorised users are only to access data and run programs that they are authorised to use; the unauthorised use of software, including the unauthorised reading, modification and deletion of data, may constitute a breach of these rules.

Authorised Software

Authorised users are to load and run only software that has been properly purchased, licensed and supplied by Government of Malawi for use on its IT Systems. Under no circumstances are users to install, record or run unauthorised programs (including unlicensed software, privately obtained software, games and screen-savers).



Authorised Hardware

Authorised users are not to modify, change or otherwise alter the hardware configuration of any Government of Malawi IT System, without the prior approval of the relevant system manager. Under no circumstances are users to install, connect or use unauthorised connections and / or communication devices between Government of Malawi and / or third party IT Systems.

Access Control

All Government of Malawi IT Systems should be protected from unauthorised use by the application of an approved access control program or facility. Authorised users are to select personal passwords comprising at least six characters (which do not form a name, characteristic of the user or easily guessed word), and users are to change in-use passwords at least once per month. Authorised users are responsible for the security of their password(s), which are not to be divulged to any other person.

Whenever in use PCs and Workstations are left unattended, authorised users are to either log-out of the system or activate an approved password protected screen-saver.

Virus Controls

An approved and correctly configured and updated anti-virus software should protect all Government of Malawi IT Systems; authorised users are not to deactivate such controls.

Authorised users are responsible for ensuring that all recording media and software received from third parties (other than previously unused media obtained from the manufacturer) is virus scanned using approved software, prior to it being used on any Government of Malawi IT System.

Back-Up

Authorised users of PCs and Workstations should back-up locally recorded data as often as is necessary to facilitate the recovery of that data in the event of a local system failure. The frequency of back-ups should be dictated by the rate of change of the locally recorded data: a back-up should be made immediately after any major data changes.

Locally recorded data on PCs connected to networks and Workstations should be backed-up to the relevant file server, whilst data recorded on stand-alone systems should be backed-up to tape-drives, diskettes or other removable storage media. Removable storage media used to record back-ups should be stored either off-site or in a fireproof safe. The system operators will take back-ups of data recorded on network servers.



Protection of Removable Storage Media

Authorised users are responsible for the security of removable storage media used on their System(s). All such media should be marked with a unique reference number, colour coded according to the classification of the recorded data and secured when not in use.

Internet Use

Authorised users who require access to the Internet, or any other public communications network, for their work should submit an appropriate application and supporting business justification to their line and system managers. Where such access is approved, authorised Internet users will be connected by the GWAN. When using the Internet, authorised users must use such access for Government purposes only, use approved Internet access mechanisms only, virus check all incoming mail and files, and take care to prevent the transmission of sensitive Government information from the Government's IT Systems onto the Internet.

Authorised users should note that, the accessing, downloading or distributing of material via Government of Malawi's IT Systems that is pornographic, racist, sexist, illegal, discriminatory, or likely to cause offence, is a disciplinary offence which can lead to removal of external network access rights, summary dismissal and / or criminal prosecution.

Removal of IT Equipment

Authorised users are only to remove IT Systems (including Personal Computers (PCs), laptops and notebooks) from Government of Malawi premises with the prior written approval of their Principal Secretary. Users authorised to remove IT equipment for home or remote work are responsible for the physical security of the System away from Government of Malawi premises, and the Government reserves the right to seek recovery of any loss attributable to the user's negligence.



Guidance and Training

The majority of IT system faults and non-availability is attributable to errors by authorised users and operators. Whenever authorised users are in doubt about the correct use of an IT System, including any constituent hardware or software component, they should seek guidance from their System Security Officer. Whenever necessary, appropriate training should be provided.

Disciplinary Action

These rules form part of all authorised users terms and conditions of employment. Failure to observe the rules may result in disciplinary action against the person(s) responsible. All authorised users should be aware of their responsibilities under the Malawi Public Service Regulations.

Declaration

I have read and understood the IT Security Code of Practice and undertake to comply with the related security requirements.

Signature: _____

Name: _____

Date: _____



INTERNET SECURITY CODE OF PRACTICE

System users are individually responsible for understanding and applying both the system security policies and procedures for the Government of Malawi information systems that they are authorised to use. System users are individually accountable for their own behaviour, both in using the Government of Malawi's own systems and those belonging to third parties that are accessed from the Government of Malawi's systems.

System users are responsible for effectively employing available security mechanisms and applying defined security procedures, to protect the Government of Malawi's data and systems. Internet access to and from the Government of Malawi systems is to be via authorised communications links only; these will be via an approved Internet Service Provider (ISP) and, for GWAN systems, via the approved firewall. (The majority of Government users will be connected to the GWAN.) The unauthorised connection of the Government of Malawi systems, whether networked or standalone, to a non-approved ISP is strictly prohibited. Authorised system users are not to share their system and / or Internet service access authority with other the Government of Malawi staff or visitors.

System users communications, both internally and externally, must not be inflammatory, harassing, defamatory, and disruptive to other's operations or otherwise reflect adversely on the Government of Malawi's reputation or image. Spamming (unsolicited advertising mail) and flaming (derogatory messages) are expressly prohibited.

System users are to be aware that Internet communications are public broadcasts, and that there can be no expectation of privacy for such messages, whether commercial, professional or personal. Information passing through the Government of Malawi firewalls to and from the Internet may be intercepted and or monitored by appropriately authorised GWAN system operations staff; the Government owns all information processed on its systems and monitors communications in order to police the application of this Code.

Classified Government of Malawi information is not to be forwarded over the Internet, unless an approved encryption facility is in use. Information integrity cannot be assumed for information obtained over the Internet and, unless verified, such information is not to be used for critical applications. Furthermore, the timeliness and general availability of information obtained over the Internet cannot be assured and should not be assumed.

Acceptable Business Uses

Authorised Government of Malawi system users may use the Internet for:

1. Government related business,
2. Communications and exchanges of public information for professional development, including with professional associations, and
3. Professional activities, including research and development, on any public domain work related activity, product or service.



Unacceptable Business Uses

The Government of Malawi staff are not to use access to the Internet for:

1. Activities not sanctioned by the Government of Malawi, or
2. For private or personal business.

The Government of Malawi staff are not to exceed their defined authority for originating external communications, including statements of policy and Government opinion and directions to suppliers and customers. Government of Malawi staff are individually accountable for the content of all electronic communications originated from their user account.

Government of Malawi staff are not to automatically forward *internal* e-mail and other electronic communications to Internet or other external addresses, unless specifically authorised to do so.

Illegal and Unethical Uses

Government of Malawi staff are not to use Government access to the Internet for:

1. Seeking to gain unauthorised access to Internet resources,
2. Wasting of any human, computer and / or communication resources,
3. Unauthorised alteration and / or destruction of any computer data,
4. Compromising the privacy of other users or data confidentiality,
5. Viewing, down-loading and / or forwarding racist or discriminatory data,
6. Viewing, down-loading and / or forwarding pornographic images,
7. Communication information about terrorist activities,
8. Communicating libellous information about third parties,
9. Playing computer games,
10. Propagating chain letters, and
11. Electronic harassment of any kind.



Anti-Virus Measures

Any software obtained over the Internet must be obtained in source code form and be inspected for potential malicious code (viruses); software available only in compiled (binary) form is not to be downloaded or used on the Government of Malawi systems.

Any attachment to files are to be virus-checked before being invoked, unless this task is automatically performed by the relevant network / e-mail anti-virus product. Users should be aware that anti-virus products will not detect malicious code in compressed files; therefore, such files need to be expanded prior to being virus-checked.

Games, screen-savers, bit-map files, video and sound clips, and other non-business related executable files are not to be downloaded from the Internet.

Reporting of Security Breaches

Authorised Government of Malawi Internet users are to report any actual or suspected breach of the Internet Security Code of Practice, and / or of the relevant System Security Policy and Procedures, to the appropriate System Security Officer.

Declaration

I have read and understood the Internet Security Code of Practice and undertake to comply with the related security requirements.

Signature: _____

Name: _____

Date: _____



LOGICAL ACCESS CONTROL

Authentication

1. A valid User / Operator ID and password should be required for all system and network access
2. User / Operator IDs should follow a standard naming convention, which facilitates the independent identification of the owner
3. Defined password formats should be used:
 - a. Administrator (super-user / supervisor) and security application (e.g. firewall) passwords should have an enforced secure format (e.g. 8 alphanumeric characters, including at least 2 numbers), and
 - b. User passwords on business critical systems should have an enforced secure format, whilst those on other systems may be of a less secure standard.
4. Passwords should be changed regularly, at defined intervals (e.g. monthly, 3-monthly)
5. User passwords should not be recorded or written down in such a way that an unauthorised person might discover them
6. Administrator passwords should be recorded and held under secure conditions by a nominated Principal Secretary

Access Privileges

1. System and network owners should authorise the allocation of all user / operator access privileges, using a defined process.

Access Administration

1. System and Network IT Managers should be notified of new starters, leavers and staff transfers before they occur, using a defined process; and
2. A special process should exist to assure the prompt removal of all access authorities and privileges for staff who are either made redundant or otherwise constitute a potential risk to Government of Malawi computer systems and communication networks.



Housekeeping and Audit

1. All access accounts and privileges should be reviewed at least once per month to facilitate the prompt removal of redundant access authorities
2. All user access rights should be reviewed and confirmed with the system, network and / or business process owners at least once every 12 months.



NETWORK SERVICES

The functionality of the GWAN should be limited to that necessary to meet defined and approved network performance and security requirements. When necessary, specialist advice should be obtained to assist in the development of secure configurations.

System and Network Connections

1. All connections between Government of Malawi systems and between Government of Malawi systems and third party systems (including public access facilities) should be subject to the prior approval of the Government Security Officer.
2. Internal Government of Malawi networks should not be visible to the public or third party systems, either by probing or through Domain Names Server (DNS) information.
3. Government of Malawi internal networks should be configured to use a class of IP addresses that are not routable over the Internet.
4. Each network perimeter server should only perform one function (e.g. firewall, web, ftp, e-mail, DNS) and be configured as an independent domain, with no trust relationship with any internal domain.

Routers & Hubs

1. Routers, switches and hubs should be located in a physically secure location, which meets the following criteria:
 - a. A locked wiring cabinet / cupboard / room, or a secure computer room
 - b. Wiring is fitted in such a way that minimises the risk of accidental damage
 - c. Access control keys are only available to the designated network administrator
 - d. The environmental conditions are consistent with the equipment vendor's requirements
 - e. The location has its own fire detection system, or is covered by an adjacent one



2. The router configuration strategy should be dictated by whether or not the connected network segments can be trusted:
 - a. *Untrusted* network segments should be configured in accordance with the security philosophy of “restrict everything unless expressly permitted”, and network traffic should require a form of authentication on the systems across the router. Network traffic transmitting confidential data and/or User / Operator IDs and passwords should be encrypted to prevent sniffing attacks.
 - b. *Trusted* network segments should be configured in accordance with the security philosophy of “allow everything unless expressly restricted.”
3. Router password security should meet the following minimum standards:
 - a. Passwords should comply with the Logical Access Control policy; and
 - b. The “secret password” feature should be used on all CISCO® routers, which enables encrypted administration passwords (similar features should be applied on other router types, if available).
4. Router change control procedures should meet the following minimum requirements:
 - a. Router configuration documentation should be current and include relevant IP address descriptions, filtering rules, the justification for the filtering rules and evidence of IT security management approval.
 - b. IT security management should approve all changes to router configurations.
 - c. Access to router configuration documents should be restricted to network administrators only.
5. Change logs should be retained and record: the nature of each change, the reason for each change, evidence of change approval, the details of the person performing a change and the date and time of each change
6. Router configurations should be compared against the approved router documentation on a 6 monthly basis, to detect unauthorised or unintended changes. Evidence of such reviews should be recorded in the change control log.
7. All routers and hubs should be protected with an Uninterruptible Power Supply (UPS).
8. Network wiring should be adequately protected to prevent accidental damage and a consequential loss of network services.

Gateways

1. Each network connection outside of the Government of Malawi should be classified as fully trusted or non-trusted.
2. The Government of Malawi network connections to non-trusted systems should be terminated at an approved firewall located on the network segment containing the



Government of Malawi system involved in the data exchange; the system should be located on the firewall's De-Militarised Zone (DMZ).

3. Network Address Translation (NAT) should be used when connecting Government of Malawi networks to external systems, to prevent disclosing internal network addresses.

VPNs

1. A Government of Malawi approved VPN should be established between component parts of the Government of Malawi Government network wherever public and / or shared network communications are used. One of the following security solutions should be applied:
 - a. A firewall to firewall VPN, if the system users can accept the related firewall performance degradation; or
 - b. A third party point-to-point VPN, which provides good performance at extra cost.

Firewalls and Proxies

1. The Government of Malawi Government network segments that need to be connected to non-trusted (external) networks should be protected by an approved firewall.
2. All publicly accessible devices (e.g. web-sites, mail servers, etc) shall be installed in a DMZ on one of the firewall's interfaces. Internal devices should only be accessible from outside Government of Malawi using a VPN and strong authentication.
3. No devices should be installed between the external router and the firewall, other than approved Intrusion Detection Software (IDS).
4. Firewall configurations and structure should reflect the following policy:
 - a. Deny any service unless it is expressly permitted;
 - b. Use restrictive packet filtering;
 - c. Filter IP addresses based on source IP address, destination IP address, TCP source port and TCP destination port.
5. Firewalls should disallow packets originating from outside the host network component, which have host source addresses, to prevent spoofing attacks. Packets received from an external source with an internal source address should be investigated.
6. Packet filtering rules should drop any packet that has any IP option set (e.g. sourceroute) to prevent the circumvention of firewall router settings.



7. Packet filtering should be used to restrict certain activities to specific servers in the perimeter network; specifically:
 - a. E-mail traffic should be restricted to the IP of the email gateway server, and
 - b. WWW traffic should be restricted to the IP of the public web server.
8. Firewalls should be programmed to block NFS packets in any direction.
9. All services should be denied at the firewall unless expressly approved by the Government Security Officer to meet an approved business need: this includes IP, Java, Active X, Cookies, tftp, RPC, Telnet, ftp, talk, IRC, RIP, SNMP and ICMP).
10. The use of a proxy is recommended for services that Government of Malawi may wish to control beyond simple deny/allow restrictions.
11. The configuration of firewalls should be reviewed independently on an annual basis.
12. Firewall administrators should monitor the configurations and settings of each firewall to ensure that it has not been incorrectly reconfigured due to error, crashes, or hacker attacks. The administrator should review the following on a monthly basis, for inappropriate changes or modifications: router configuration tables, firewall server configuration settings, other server configuration settings that are located in the DMZ, and proxy server configuration settings and proxy rules
13. User account listings for each firewall component should be reviewed on a quarterly basis to determine the validity of existing accounts. Components of the firewall should limit the number of accounts used for administration. All default vendor-installed accounts and passwords should be disabled or deleted. Two accounts may exist on each component, an account for the firewall administrator and his/her backup. Extreme care must be taken when assigning passwords to these accounts.
14. Wherever possible, carefully defined content filtering should be used to minimise the risk of unauthorised code and commands being introduced to Government of Malawi networks from outside.
15. A firewall should also be provided to restrict access between elements of the Government of Malawi network to help assure privacy and segregate systems and network components with different risk profiles.
16. Firewall management console(s) should be located within a physically secure area with access limited to authorised IT staff only.



Internet Connections

1. Separate Internet connections should be maintained for e-mail and other services.
2. The number of Internet connections should be kept to the minimum consistent with the cost-effective provision of approved services. The configuration of Internet connections should be such that any related performance degradation does not impact on other services.
3. Internet access and services should be kept to the minimum consistent with approved business requirements (e.g. relay-chat, news-group access).
4. Firewalls installed to protect Internet connections should be configured to require two-factor authentication by authorised users, including a password, prior to establishing external communication. This is necessary to both control Internet access in general and to provide an audit trail of Internet activities positively assigned to specific users.
5. An audit trail of Government of Malawi users Internet activities should be maintained and reviewed periodically to assure compliance with the Acceptable Use policy.
6. Internet connections should be protected by an approved IDS.

Internet Sites

1. Government of Malawi web-sites accessible over the Internet that contain Confidential or Internal Use Only information should be configured to communicate using SSL, or another Government of Malawi approved encryption process. Access to these and other restricted areas of Internet connected web-servers should require strong User ID and password access control.
2. An integrity-checker should be installed on Internet connected web-sites and configured to provide an alarm whenever unauthorised changes are made to the site's configuration.
3. Specialist advice should be obtained on the secure configuration of web-servers and applications, due to the large number of potential security design vulnerabilities.



Dial-Out

1. Government of Malawi will provide IT users with access to external systems and networks, including the Internet, where there is a business case and using secured gateways. Most if not all users requiring Internet connectivity will connect via the GWAN infrastructure.
2. Dial-out access and modems should not be installed on PCs and workstations.

Remote Access

1. Remote access facilities are a primary source of system and network vulnerability. The Government Security Officer and relevant Business Process / Information Owner should determine whether remote access to their systems is necessary. Users should only be granted remote access with the written authorisation of their Principal Secretary. Users requiring remote access to e-mail only should be denied access to other services. Such services should only be provided where there is a compelling business case and appropriate security measures are taken, including:
 - a. Two-factor authentication for non-critical systems; and
 - b. Strong two-factor authentication for critical systems and networks.
2. Where remote access facilities are used for administrator (super-user / supervisor) access to Government of Malawi systems and / or to access systems used to process confidential information, the remote access communications should be encrypted.
3. Wherever remote access is approved, it should be made available via a secured gateway or firewall. Government of Malawi staff should only operate approved remote access services using hardware and software supplied by Government of Malawi.
4. The list of authorised remote users should be reviewed regularly to confirm a continuing business need and the use of remote access facilities should be monitored for suspicious or unauthorised activity.
5. Where essential, remote access to Government of Malawi systems, networks and information by third parties may be approved, provided it is governed by a formal agreement, which specifies appropriate security requirements.



6. Only one remote connection to the Government of Malawi GWAN should be permitted for each user ID at any one time.
7. Remote maintenance facilities should be strictly controlled and protected by the same authentication standards as are required for other forms of remote access. Remote access facilities used by contractors and other third parties should be protected by:
 - a. Government of Malawi retaining control over the allocation of access accounts, privileges and authentication controls (including passwords)
 - b. The activation of the communication link for agreed maintenance activities only
 - c. The physical and logical disconnection of the communication link when not in use.

Malicious Code

1. All imported media should be virus checked before the data is imported onto Government of Malawi systems, and all e-mail attachments should be virus checked before being opened or distributed.
2. To automate anti-virus protection, approved anti-virus software shall be installed on:
 - a. All Government of Malawi systems, including networked workstations and servers; and
 - b. On all e-mail gateways between Government and public / shared networks.
3. Installed anti-virus software shall be continuously enabled, configured for the real-time detection and reporting of viruses, and updated promptly as and when recommended by the developer. The unauthorised re-configuration of anti-virus software is strictly forbidden.
4. There should be a well defined local process for the reporting of virus infections.
5. Users should not attempt to remove viruses from infected systems themselves.

Encryption

1. The Government of Malawi confidential and Internal Use Only data sent over public and / or shared communication networks should be encrypted using an approved process; four common circumstances require different encryption solutions:
 - a. E-mail messages and / or attachments to internal and / or external addresses
 - b. Remote access to Government of Malawi systems used to store / process Confidential data
 - c. Viewing confidential Internet Web-pages



- d. Using public (e.g. Internet) and / or shared communication networks as part of the Government Wide Area Network.
2. Encryption processes should not be used or applied to Government of Malawi data, unless the process (es) have been formally approved.
3. Approved encryption processes should use 40-bit keys.
4. Where approved encryption processes involve the allocation of private keys, Government of Malawi users should safeguard their keys(s), pass-phrases and / or digital certificates and make them available to the Government Security Officer when there is a business need and on leaving the Government.
5. The Government Security Officer should issue details of approved encryption processes and guidelines for their use.

FTP

1. FTP should not be used unless there is a compelling business justification. If essential, an FTP server should be provided and configured for:
 - a. Posting files individually secured using an approved encryption process, with User ID and password access control
 - b. Access via either Secure Hyper Text Transfer Protocol (SHTTP) or Secure Sockets Layer (SSL), together with User ID and password access control, or
 - c. Access via an approved Virtual Private Network (VPN).
2. Anonymous FTP access and Trivial File Transfer Protocol (TFTP) should be disabled.

Telnet

1. Telnet sessions to and from Government of Malawi systems should not be enabled or used, other than over an approved VPN.

Software Licensing

1. Formal approval should be obtained from Government of Malawi IT management prior to installing any software on Government of Malawi systems and networks.
2. Third party software installed on Government of Malawi systems is to be legally obtained from approved reputable source(s) and correctly licensed.
3. Compliance with this policy should be assured via the periodic auditing of software installed on Government of Malawi systems and associated licensing agreements.



Physical Security

1. Government of Malawi owned systems and network components should be:
 - a. Permanently and uniquely marked as Government of Malawi owned assets;
 - b. Located and operated within a managed security perimeter inside Government of Malawi or trusted third party premises
 - c. Positioned away from potential hazards, including over-head water and heating systems / pipes and flammable materials
 - d. Protected by a filtered power supply and other appropriate environmental controls
 - e. And, if essential to business critical operations, covered by a stand-by power supply
2. Desktop systems and all storage media are to be physically protected from unauthorised access, when not in use, by at least one level of approved lock.
3. Laptops and desktop computers delivering core satellite applications should be physically secured when not in use, have the power-on password activated and kept separate from any authentication tokens.
4. Servers and communication facilities should be housed in dedicated secure accommodation with access limited to designated and appropriately qualified IT staff.
5. Positive physical control should be exercised over staff, contractor and visitor access to, and activities within, areas that house business critical and / or security significant Government of Malawi system and network components.
6. All Government of Malawi Confidential and Internal Use Only electronic data should be encrypted when not protected by suitable physical protection measures.

Personnel Security

1. All Government of Malawi system and network users and operators, including management, should receive appropriate training in the use and operation of the hardware and applications.
2. All new Government of Malawi staff should attend a security awareness briefing and be required to read and sign:
 - a. Terms and conditions of employment, requiring them to preserve the confidentiality of Government of Malawi information and to comply with Government of Malawi IT security policies
 - b. A confidentiality agreement covering Government of Malawi information



3. Disciplinary procedures should be defined for users who are found to be in breach of these security policies, or who are found to be engaged in computer misuse.

Security Monitoring

1. The audit trail facility on operating systems and security significant applications (e.g. remote access servers, firewalls, anti-virus tools, intrusion detection software) should be active and record:
 - a. Failed log-on attempts;
 - b. All changes to administrator (super-user / supervisor) access authorities;
 - c. System commands issued by administrator accounts;
 - d. External communications; and
 - e. Other potentially significant security related events.
2. Log files produced by active audit trails on business critical systems should be reviewed at least once each normal working day and, thereafter, archived for one month. Records of unauthorised and / or unexpected events should be fully investigated.
3. Where an audit trail relates to a key security mechanism (e.g. Internet firewall) on a business critical system, the audit log should be monitored in real-time on a dedicated terminal incorporating an alarm facility for significant events.

Security Assurance

1. Procedures should be in place to assure the reporting and escalation of security incidents, as and when they are discovered.
2. Clocks shall be synchronised on all systems to assure log accuracy in the event of a security incident and for valid evidential purposes.
3. Periodic audits should be performed to assess compliance with both this policy and local legislation. Audits should be performed on both a national and regional basis to adequately assess compliance.

Contingency Arrangements

1. Back-up copies of in-use data and applications should be taken at appropriate intervals and stored securely, to protect against the accidental / deliberate loss of the in-use media:
2. Individual users should be responsible for backing-up their own data stored locally on PCs and workstations;



3. Relevant IT personnel should be responsible for backing-up network servers and communication devices, either completely or incrementally;
4. The frequency of back-ups should be such that an up-to-date version of the in-use data can be created from the latest back-up copy in an acceptable manner;
5. Back-up copies should be stored either in a fire-proof safe within the same building as the in-use media or in a secure location in another building; and
6. The ability to recover from back-ups should be tested periodically.

Maintenance

1. Government of Malawi systems and network components should undergo regular maintenance by approved personnel.
2. External maintenance personnel servicing Government of Malawi system and network components should be supervised by a trusted member of Government of Malawi staff throughout their work.
3. A detailed record should be maintained of all internal and external maintenance activities.



VIRUS PROCEDURES

1. Responsibilities for virus protection will be clearly assigned and training provided where appropriate.
2. All staff will comply with *Virus Procedures* which include the need to:
 - a. Switch off machines each night so that the automatic virus scanner will activate when machines are next switched on:
 - b. Be on the alert for unsolicited or suspicious emails, files or software and, if in doubt, to seek specialist help;
 - c. Promptly report virus infections; and
 - d. Check removable media (diskettes, CDs) on using approved virus scanning software before they are used on Government of Malawi systems and before they are sent to clients or other third parties.
3. Software will only be loaded by authorised server, gateway or desk-top support functions.
4. Only properly licensed software from reputable sources will be used on Government of Malawi systems.
5. All software (including shrink-wrapped software) will be virus checked prior to installation.
6. The Government will not deploy IT systems incapable of supporting anti-virus products.
7. Effective anti-virus products will be employed to detect and remove viruses on all workstations, servers and gateways. In particular:
 - a. Anti-virus electronic mail gateways will be used to virus check all internal mail and messages sent and received from external mail services;
 - b. Anti-virus products will be used on all connections to external services and networks.



8. Virus checking will cover all outgoing and incoming messages. Where necessary, multiple anti-virus scanning products will be used to provide protection against a wider range of viruses than would be possible with a single product.
9. The effectiveness and suitability of anti-virus software will be monitored. Anti-virus products will be kept current and deployed once the business is confident of the product's stability.
10. All anti-virus products will be consistently configured for the real-time detection and reporting of viruses. Unauthorised re-configuration of anti-virus products is strictly forbidden.
11. Remote access to Government of Malawi systems, networks and information by third parties (including vendors) will be covered by formal agreements, which specify required security procedures. These agreements will require third parties to comply with the principles of this policy.
12. All computers (lap-tops and desk-tops) used by staff for company business outside of Government of Malawi's offices will be supplied by Government of Malawi to a standard configuration, which includes anti-virus software. Where staff use these machines for remote access, the Remote Access Security section of this document will be complied with at all times.
13. Government of Malawi's offices, clients and other third parties will be:
 - a. Advised that, although material sent out has been virus scanned, they should undertake their own checks prior to use; and
 - b. Notified of all viruses received from them and warned of viruses, which may have been sent to them inadvertently.
14. IT systems will be virus checked following system up-grades, maintenance or prior to commissioning the system to the production environment.
15. Information, applications and operating systems will be backed up regularly in such a way that it is possible to revert to a virus free state following an infection.
16. Updates to anti-virus products will be automatically distributed to users upon logging into the LAN servers.



APPENDICES

Information Security Terms

Term	Explanation
Acceptable risk	<p>By quantifying acceptable risk in the same terms as actual risk, attention can be focused on information resources that pose a level of risk beyond that regarded as acceptable.</p> <p>Acceptable risk can be expressed quantitatively by setting the:</p> <ul style="list-style-type: none"> ❑ controllable components of risk (i.e. control weaknesses, level of threat and business impact) to values regarded as acceptable by top management (erg zero control weaknesses, fewer than 10 incidents a year, no business impact greater than 'minor') ❑ non-controllable components of risk (i.e. criticality and special circumstances) to meaningful threshold values (e.g. the average level of criticality across a group of information resources; the average number of special circumstances that apply to such information resources).
Availability	<p>Availability is the property of information being accessible and useable when required by the business. It has two aspects:</p> <ul style="list-style-type: none"> ❑ response time: the length of time taken to respond to a business user's request for information ❑ up time: the dates and times during which the information is available to a business user. <p>In both cases, measurements should be made from a user's perspective, since this will often vary from that measured by the system manager(s).</p>
Business impact	<p>Business impact is a value or rating that indicates the nature and level of harm suffered by an enterprise as a result of an <i>actual</i> loss of confidentiality, integrity or availability of information (whereas <i>criticality</i> considers the worst-case <i>possible</i> loss).</p>
Confidentiality	<p>Confidentiality is the property of information being secret or private within a predetermined group.</p>
Control	<p>A control is a policy, method, procedure, device or programmed mechanism intended to protect the confidentiality, integrity or availability of information.</p>
Control weakness	<p>A control weakness arises when a control that is needed is either not implemented or is not applied in all cases where it should be.</p>
Criticality	<p>Criticality is a value or rating that indicates the relative importance of an information resource to an enterprise, based on the maximum level of harm that could arise if the confidentiality, integrity or availability of information was compromised, taking into account the timescale of a loss of availability.</p>
Data	<p>The representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or by automatic means.</p>
DMZ	<p>Demilitarised Zone.</p>
DoS Attack	<p>A Denial of Service (DoS) attack is a remote attack against a servers TCP/IP stack or services. DoS attacks can saturate a server's bandwidth, saturate all available connections for a particular service, or even crash a server.</p>
Effectiveness	<p>Effectiveness is the extent to which an action, process or</p>



Information Systems Security Policy

Term	Explanation
	arrangement fulfils its stated purpose.
Exploit	A script or program that takes advantage of vulnerabilities in services or programs to allow an attacker to gain unauthorized or elevated system access.
Host	A node on a network. Usually refers to a computer or device on a network, which both initiates and accepts network connections.
Information incident	An information incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of business information <i>in practice</i> . The categories of information incident that influence information risk should include those listed in the definition of threats, above.
Information resource	Information resource is a collective term for information and associated facilities. Accordingly, the relevant facilities are business applications, computer installations, communications networks and system development capabilities.
Information risk	Information risk is the chance or possibility of harm being caused to a business as a result of a loss of the confidentiality, integrity or availability of information. The level of risk associated with an information resource can be evaluated by measuring: <ul style="list-style-type: none"> <input type="checkbox"/> the criticality of the information resource to the business <input type="checkbox"/> control weaknesses affecting the information resource <input type="checkbox"/> special circumstances affecting the information resource <input type="checkbox"/> threats to the information resource <input type="checkbox"/> the business impact of information incidents experienced over a period.
Information security	Information security is a field of endeavour concerned with the protection of the confidentiality, integrity and availability of information.
Information Technology	The scientific, technological and engineering discipline and the management of techniques used in data handling and processing; their applications; computers and their interactions with people and machines; and associated social, economic and cultural matters.
Integrity	Integrity is the property of information being a correct and sound representation of an authorised business process. Integrity has three aspects: <ul style="list-style-type: none"> <input type="checkbox"/> completeness: the property of information being present in its entirety <input type="checkbox"/> accuracy: the property that information is exactly as intended <input type="checkbox"/> validity: the property that information reflects authorised business processes.
IP Address	The 32-bit address defined by the Internet Protocol in STD 5, RFC 791. It is usually represented in dotted decimal notation. Any device connected to the Internet that used TCP/IP is assigned an IP Address. An IP Address can be likened to a home address in that no two are alike.
LAN	Local Area Network
Level of threat	The level of threat indicates the likelihood of a threat or category of threat materialising. This can be evaluated based on historical incident data.
MAN	Metropolitan Area Network
Monitoring	Monitoring is an action-oriented process involving: <ul style="list-style-type: none"> <input type="checkbox"/> measuring <input type="checkbox"/> presentation of measurements to one or more decision-makers <input type="checkbox"/> initiation of remedial action <input type="checkbox"/> re-measurement to determine the effectiveness of remedial action.
Netbios	Network Basic Input Output System. The standard interface to



Information Systems Security Policy

Term	Explanation
	networks on IBM PC and compatible networks.
Owner	Individual or organization having responsibility for specified information asset(s) and for the maintenance of appropriate security measures.
Ping	A program used to test reachability of destination nodes by sending them an ICMP echo request and waiting for a reply.
Port	A port in the network sense is the pathway that a computer uses to transmit and receive data. As an example, Web Servers typically listen for requests on port 80.
Registry	The internal system configuration that a user can customize to alter his computing environment on the Microsoft Windows Platform. The registry is organized in a hierarchical structure of subtrees and their respective keys, subkeys, and values that apply to those keys and subkeys
Risk Analysis	Comprehensive concept for defining and analysing threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimise investment in security countermeasures.
Service	A service is a program running on a remote machine that in one way or another provides a service to users. For example, when you visit a website the remote server displays a web page via its web server service.
Share	A folder, set of files, or even a hard drive partition set up on a machine to allow access to other users. Shares are frequently set up with incorrect file permissions, which could allow an attacker to gain access to this data.
Sniffer	Frequently attackers will place a sniffer program on a compromised machine. The sole purpose of a sniffer is to collect data being transmitted on the network in clear-text including usernames and passwords.
Special circumstance	A special circumstance is a circumstance other than a control weakness that influences the likelihood of threats materialising (e.g. a high degree of change, complexity, accessibility by external parties).
Subnet	A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number.
Threats	Threats are the means by which the confidentiality, integrity and availability of information <i>could</i> be compromised. The categories of threat that influence information risk include: <ul style="list-style-type: none"> <input type="checkbox"/> malfunctions of software or hardware <input type="checkbox"/> loss of services, equipment or facilities <input type="checkbox"/> unforeseen effects of change <input type="checkbox"/> overloads <input type="checkbox"/> human error <input type="checkbox"/> access violations.
Vulnerability	Vulnerabilities are circumstances that increase the likelihood of threats materialising, i.e. control weaknesses and special circumstances or a weakness or a flaw in a program or service that can allow an attacker to gain unauthorized or elevated system access.
WAN	Wide Area Network



List of Abbreviations Used

Abbreviation	Explanation
CGIS	Central Government Information System
DISTMS	Department of Information Systems and Technology Management Services
EYCA	Ernst & Young Central Africa
FIMTAP	Financial Management, Transparency & Accountability Project
GoM	Government of Malawi
GWAN	Government Wide Area Network
ICT	Information and Communications Technologies
IFMIS	Integrated Financial Management Information Systems
IT	Information Technology
KPI	Key Performance Indicators
LGIS	Local Government Information Systems
OPC	Office of the President and Cabinet
PPPAI	Payroll, Pensions and Personnel & Advances Integrated System

