Republic of Zambia

Office of the President
Electronic Government Division

PUBLIC SERVICE INFORMATION COMMUNICATION TECHNOLOGY STANDARDS

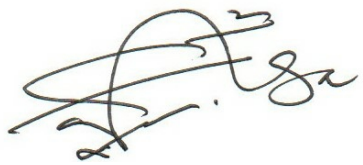
Acceptable Use Guidelines and Procedures

Foreword

The Government of the Republic of Zambia through the e-Government Division is delighted to publish the second edition of the Information and Communications Technology (ICT) Acceptable Use Guidelines and Procedures. This edition supersedes the first edition issued in 2015. This guideline sets out minimum acceptable professional behavioral standards for using various ICTs at our disposal as we are employed in the Public Service.

The Government is continuously focusing on the expansion of ICT infrastructure and the delivery of public services through multiple channels accessible to all citizens especially in rural areas. To achieve this, Government is transforming the way it conducts business to have a well-equipped and trained Public Service with appropriate tools to execute assignments diligently. Various Ministries, Provinces and other Spending Agencies (MPSAs) have increasingly embraced ICTs to enhance their operational efficiency and management effectiveness. This is commendable and should be encouraged to grow keeping in mind the need to ensure the security and integrity of the information generated, stored and transmitted.

All MPSAs are urged to continue embracing ICTs as a critical tool that reaches across boundaries to make public services available to the citizenry for a better Zambia. All Permanent Secretaries and Heads of MPSAs are directed to bring the contents of these guidelines to their respective employees to ensure full compliance for effective and efficient public service delivery.



Martine G. Mtonga (Dr.)
National Coordinator
SMART Zambia Institute

Acknowledgment

The Government of the Republic of Zambia is committed in transforming the way it interacts and delivers services to **MPSAs,** business houses and citizens. Through its various transformation efforts, the Government has identified **ICTs** as a critical component for the improvement of public service delivery.

The ICT Acceptable Use Guidelines and Procedures will ensure that ICT resources are not abused and are used for the intended purpose. MPSAs are encouraged to operationalise the provisions in this document for their operational efficiency and effectiveness in safeguarding Government ICT systems and information.

I wish to commend the e-Government Standards Task Team, Heads of ICT in Ministries, Provinces and other Spending Agencies (MPSAs) and various stakeholders for their unwavering efforts in the development of the ICT Guidelines and Procedures document.

Percive Chinyama
Director Standards
SMART Zambia Institute

Table of Contents

Abbreviations and Acronyms

ICT	Information and Communication Technology
ID	Identity
IP	Internet Protocol
IR	Information Resource
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
QoS	Quality of Service
SMS	Service Management System
VOIP	Voice Over IP
VSAT	Very Small Aperture Terminal

Working Definition

Application Incident: This is an event that makes a user fail to use an application or that produces results that are not according to the user's expectation.

Application Platform: This is the environment in which the application operates. This includes the associated computer hardware and the operating system.

Application Software: This is software used by users to perform business functions.

Application Support: This is the activity of ensuring that application systems are always available and operating smoothly.

Availability: The degree to which a system or data access suffers degradation or interruption in its service to the customer as a consequence of failures of one or more of its parts.

Bespoke (customized) Development: Bespoke (customized) development means developing systems from scratch.

Capacity Testing: This is a kind of testing that provides insights on the volume of data a system is capable of processing. This is an important parameter to be aware of as it helps in ensuring that the system is properly operated.

Cell Phone: This is a hand-held system that is used in mobile communication so as to enable a user to be in constant communication at any time and almost anywhere where there is network coverage.

Change Control: This is a mechanism established in an IT environment in which changes to the IT infrastructure or systems are monitored and controlled. The purpose of this mechanism

is to establish and maintain systems' integrity. Only approved changes that have been economically or otherwise justified are implemented and documented.

Computer Equipment: Computer equipment refers to computer systems and all related hardware.

Confidentiality: This is a security requirement that safeguards corporate data from unauthorised access and disclosure.

Disaster Recovery: This is a process of restoring to original status, damaged infrastructure, in this case ICT infrastructure, after a disaster.

Email: This is a computer service used for sending and receiving messages electronically over computer networks. An email user will be identified on the network by an email address with which he sends and receives messages.

File Transfer: Moving files from one machine to another on a network is called file transfer. Users can use the Internet to transfer computer files between their PC and just about any other computer on the Internet.

Firewall: This is an access control mechanism that acts as a barrier between two or more segments of a computer network or over all client/server architecture, used to protect internal networks or network segments from unauthorised users or processes.

Host: This refers to a computer system that provides computer service for number of users.

Illegal Application: Refers to any out-sourced application or an application developed using tools not registered with the GRZ and Information Communication and Technology Sections. This will include games that are not registered e.g., Chess, Grand Prix, etc.

Illegal Use: Refers to use of GRZ ICT resources be it hardware or software for non-GRZ business.

Information Attack: It is an attempt to bypass the physical or information security measures and controls. The attack may alter, release, or deny access information. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Information System Access Control Standards: Information System Access Control Standards are rules that are applied in order to control access to information for an organisation, say GRZ. These standards should always be appropriate to the organisation's business and security needs. The dangers of using inadequate and/or inappropriate access control standards range from inconvenience to critical loss or corruption of data.

Information Browsing: This term refers to the process of going through information on any web site. Users can use specialized software tools to browse through an almost limitless collection of information.

Information Resources: This term refers to any and all computer printouts, online display devices, magnetic storage media, and all computer related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, PCs, notebook computers, hand-held computers, Personal Digital, Bar Code Scanners, URUs, Assistants (PDAs), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Integrity: This refers to the trueness and correctness of a system and its data.

Internally Supported Out-sourced System: refers to an out-sourced system on which the vendor has allowed enhancements to be carried out by internal ICT staffs that have been trained by the vendor.

Internet Mail: This is electronic mail sent through the Internet. The Internet can be used to send e-mail to virtually any networked computer user in the world. Internet mail can be delivered anywhere in the world in a matter of minutes or at the most a few hours.

Load Testing: This is an important test as it shows how much loading a system can sustain. Toward the maximum loading, performance of the system deteriorates, thus it is important to determine the maximum loading so that the system can be operated optimally.

Local Area Network (LAN): This refers to a data communication network spanning a limited geographical area, a few kilometers at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Obscene Material: Refers to material in electronic form that is repulsive, disgusting and offensive to accepted standards of decency or modesty.

Office Systems: These are software systems that are used for general office work, such as spreadsheets (e.g., Microsoft Excel, Lotus) and word processors (e.g., Microsoft Word).

Parallel Running: Parallel Running is the process of running a new or amended system simultaneously with the old system to confirm that it functions correctly before going live.

Personal Computer Configuration Standard: This is a GRZ ICT standard for configuring personal computers. This standard is defined as a guide in the document called PC SECURITY CONFIGURATION GUIDE. This guide was derived from the perspective of securing PC and therefore emphasizes on PC security.

Pornography: Refers to sexually explicit pictures, writing, or other material existing in electronic form, which may depict nudity, sexual acts or other forms of indecent exposure.

Privacy: This refers to the protection of data such that the data is accessible to authorised users only.

Risk Management: This is a process that includes identification, assessment, and mitigation of probabilistic security events (risks) in information systems to a level commensurate with the value of the assets protected.

Security Incident: In information operations, it is an assessed event of attempted unauthorised entry, or an information attack on an automated information system. It includes unauthorised probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Server: A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Software: Anything that can be stored on a computer disk is software. This includes programs and data.

Software Code: This is a set of instructions that form a computer program written to perform a given logical function. The computer processor interprets these instructions.

Software Testing: This is a process used to establish that the software product meets the requirements. The test is conducted against benchmarks that are drawn from user requirements, system specifications and general standard requirements of the given system.

Source Code: These are computer instructions that are human readable and are usually written by humans (programmers) in plain text.

Stress Testing: This is a kind of testing that is carried out to see how a system can perform under abnormal conditions.

System Development: Refers to an IT function that deals with the development and acquisition of business solutions.

System Incident: This is an event that makes a user fail to use a system or that produces results that are not according to the user's expectation.

System-level Account: Refers to an access account that is for the administration of an application (e.g., Oracle database administrator and administrator accounts).

System Owner: A system owner is a person who has overall responsibility for operating a given system. For the purpose of accountability, it is important that the owner of the system is stated.

System Software: System software is a program that controls computer hardware, e.g., an operating system like Windows.

System Support: This is the activity of ensuring that systems are always available and operating smoothly.

Third Party: This refers to personnel other than the organisation's staff who is engaged to work with that organisation on some projects.

User-level Account: Refers to an access account for a person who uses a system to perform a business function.

User Requirements Specification: This is a definition of what the user of a system to be built expects. This is presented in form of a document. Usually there is need to sign of the user requirements specification to authenticate that they are agreed specifications between the user and the system developer.

Vendor: This refers to a seller of ICT services or products.

The term is used broadly to address a range of established and relatively new technologies, among which are:

a) **Information technology (IT)** which uses computers that have become indispensable in many organisations to process any volume of data and save time and effort.

b) **Telecommunications technologies** which include telephones (with fax) and the broadcasting of audio and visual data through various means including satellites.

c) **Networking technologies** of which the best known is the Internet, but which has extended to mobile phone technology, Voice over IP telephony (VOIP) and satellite communications.

Document Information

File Name	Systems Development and Acquisition Standards
Document Description	Provides compliance requirements for Standards Governing Human Capital Development, in Government
Original Authors	ICT Standards Technical Task Team
Creation Date	August, 2018
Last Update	February 2019
Report Number	1
Version	Version 2.0 (F)

Document Approval

NAME (BOARD OF DIRECTORS)	TITLE	DATE
Dr. Martine G. Mtonga	National Coordinator	
Mr. Percive Chinyama	Director - Standards	

Document Distribution

NAME	TITLE	ORGANISATION
Dr. Martine Mtonga	National Coordinator	Smart Zambia
Mr. Percive Chinyama	Director - Standards	Smart Zambia
Mr. Milner Makuni	Director - eGovernance	Smart Zambia
Stakeholders	Directors and Managers	MOCT and ZICTA All
Heads of ICT	Heads of ICT	All MPSAs

Document History/Record of Updates

DATE	AUTHOR/S	VERSION	DESCRIPTION
August, 2018	ICT Standards Technical Task Team	Issue 1.0 (D)	Produced by e-Government Division
February, 2019	ICT Standards Technical Task Team	Issue 2.0 (F)	Produced by e-Government Division

CHAPTER 1

1.0 INTRODUCTION

Various ICTs are distributed to Public Service Institutions to support the efficient and effective delivery of their mandates. However, due to the size and geographical distribution of the Public Service, Government faces challenges in the security, usage, maintenance, disposal and obtaining value for money of the various ICTs deployed for use by designated officers.

The ICT Acceptable Use Guidelines and Procedures serves to provide a standard for the acceptable use of ICT infrastructure across the Public Service. This document shall be reviewed once every three (3) years but could be updated whenever necessary to ensure the productive use of all ICTs for the purpose of enhancing Public service delivery. The e-Government Division shall set and enforce ICT standards and guidelines across all aspects of ICTs which include systems, infrastructure, processes, human resources and technology in the public service.

The e-Government Division and key stakeholders shall be accountable and responsible for recommending updates and changes to the ICT guidelines and procedures as and when required. The Division shall delegate officers responsible for ICTs in MPSAs to ensure that all organisational units, employees, consultants, contractors, and any other third parties with access to GRZ ICT resources are aware of the ICT Guidelines. The guidelines shall specify the minimum approved Government specifications and provide technical guidance for MPSAs when deploying ICTs.

These guidelines shall be implemented along with other existing polices, guidelines and standards in the Public Service. MPSAs must fully understand their obligations to effectively manage Government ICT system. The operations of ICTs should follow the guidelines set out in this document to ensure the optimal usage of ICTs across the Public Service.

This document sets out guidelines for security, acquisition, support and disposal of ICT systems in MPSAs.

1.1 Background

ICT describes various technologies that make information and communication services available to a wide range of users.

MPSAs shall use ICTs as a key driving element for achieving productivity goals efficiently and effectively.

However, it should be noted that there are risks, which come with the use of ICT. This implies that Government of the Republic of Zambia (GRZ) should balance the benefits and the risks of expanded ICT use in a way that is consistent with its corporate goals. Recognizing the critical importance of ICT and its risks, this document presents the guidelines and procedures that should govern the use of ICT in GRZ.

1.2 Objectives

This ICT acceptable use guidelines and procedures seeks to address the productive use of ICTs, potential threats and vulnerability to information systems in the public service. The GRZ ICT guidelines and procedures are based on the current and future needs for productive use of ICTs, potential threats and vulnerabilities to information and data stored on GRZ computers. Information and data must be utilized, secured in a way that ensures its integrity, availability and confidentiality. The following objectives have been drawn:

a) To enhance the utilization and support of ICTs in the public service;

b) To protect all critical information from unauthorised access and disclosure.;

c) To provide management in MPSAs with direction and support for ICT utilisation; and

d) To promote monitoring and evaluation for infrastructure and information communication services.

1.3 Scope

The guidelines and procedures contained in this document shall accordingly apply to all MPSAs' employees, contractors and consultants for them to have access to and/or using public ICT resources, administering public ICT resources, storing any non- public ICT resources, and dealing with requisition, procurement, replacement, and upgrading of ICT resources.

The Acceptable Use guidelines and procedures will also apply to all Public ICT Resources currently in existence and to any new automation technology that will be acquired in future, at all levels of sensitivity, whether maintained in-house or commercially. These ICT resources include but are not limited to: government information; applications (all software both out-sourced and in-house developed applications); and ICT infrastructure.

1.4 Enforcement

The ICT Acceptable Use guidelines and procedures document shall be read with other existing legislation, Public Service management policies, procedures and guidelines, administrative circulars and instructions issued by the relevant authorities. Repercussions for violating any of the clauses specified in the guidelines and procedures contained in this document shall be given depending on the type of offence and offender as follows:

a) **Staff**: Disciplinary action shall be in accordance with the GRZ Disciplinary Code;

b) **Contractors and consultants:** Violation may cause review of engagement contract; and

c) **Students**: Violation shall result in termination of industrial attachment.

CHAPTER 2

2 ICT HARDWARE AND OTHER EQUIPMENT GUIDELINES

2.1 ICT Equipment Acquisition

2.1.1 Overview

The purchase of ICT Hardware and other Equipment requires careful consideration in line with an organisation's business needs. It must be understood that the rate of technological changes in this area is very high. Poorly defined business requirements would result in purchasing low specification ICT equipment, which would be obsolete within a short time of usage. It is important that acquisition of this equipment is centrally managed through the ICT Sections in liaison with the procurement unit to ensure that uniform minimum technical specifications are adhered to and all relevant procedures e.g. Authority from the Plant Vehicle and Equipment Committee (PVEC) is acquired.

2.1.2 Purpose

The purpose of this guide is to ensure that the acquisition of ICT Hardware and other Equipment is done properly in order that only equipment that meets the requirements of GRZ is purchased.

2.1.3 Guideline Statement

1. Only ICT hardware and equipment that complies with GRZ's ICT Minimum Technical Specifications issued by the Office Equipment and Machine Services and other related international standards shall be purchased.

2. Acquisition of all ICT Hardware and other ICT equipment shall be done according to the laid down procurement procedures pursuant to the Zambia Public Procurement Authority (ZPPA) Act.

3. All ICT Hardware and other ICT equipment purchases shall be based on the approved work plan and budget and technical specifications that are drawn by the ICT Sections. A technical evaluation should be undertaken to ensure that the equipment is fit for its intended purpose and duly Type Approved by the Zambia Information and Communications Technology Authority.

4. All Heads of ICT Units shall be involved in the technical evaluation and inspection process of all ICT Equipment procured by MPSAs and update the ICT Equipment Returns for that particular MPSA.

5. The ICT Unit Shall test the equipment before it is installed for use.

6. All donated ICTs must meet the stipulated Government minimum technical specifications as issued by the Office Equipment and Machine Services

7. Only qualified personnel must be allowed to install ICT equipment and maintenance of equipment shall only be carried out by authorized individuals.

8. ICT equipment should be operated within recommended environmental conditions e.g. temperature, humidity, etc.

2.2 Installation of ICT Hardware and other Equipment

2.2.1 Overview

ICT Hardware and other equipment provide the platform on which software systems are implemented. The software installed on the hardware determines the overall application for that hardware. In this regard the installation of this hardware should be properly planned to avoid unnecessary disruption of services and to ensure that information security issues that may arise are adequately covered. This guideline establishes the concerns in new installations.

2.2.2 Purpose

The purpose of this guide is to ensure that all ICT Hardware and other equipment are installed properly, with the correct configuration settings.

2.2.3 Guideline Statement(s)

All ICT Hardware and other equipment installations are to be done by designated ICT staff only and according to laid down GRZ procedures. The hardware and software that must be installed shall meet the GRZ ICT minimum technical specifications.

2.3 Communications Systems

2.3.1 Overview

Communication systems form the backbone of voice and data transmission systems. Some of the applications that may use the communication infrastructure are sensitive to the quality of service (QoS) that can be offered by the communication systems. The data being transmitted over communications systems requires to be secured.

2.3.2 Purpose

The purpose of this guideline is to outline and establish the requirements for managing the GRZ communication systems.

2.3.3 Guideline Statement(s)

1. All GRZ ICT communication systems shall be designed, configured and maintained according to the set GRZ ICT procedures. Only the GRZ ICT Sections or their duly appointed delegate is authorised to design, deploy, manage and maintain GRZ's communication systems.

2. All data within the GRZ network shall be secured according to the GRZ ICT Security specifications and in accordance with relevant National Laws on Cyber Security, Cyber Crime and Personal Data Protection and Privacy.

2.4 ICT Networks

2.4.1 Overview

Government has initiated a standard government -wide approach to the planning, design and implementation of a strategic ICT network infrastructure that supports the delivery of services and meet the operational needs of individual MPSAs. The Government Wide Area Network (GWAN) provides centralised key services such as internet access, email, voice, data, video, access control, scheduling, anti-malicious software (anti-malware), and access to a dedicated helpdesk.

The local and metropolitan networks for all MPSAs are connected to the GWAN for easy management of networks and peripheral devices. The result is an efficient service delivery network model that is robust, efficient and secure.

2.4.2 Purpose

The purpose of this guide is to outline and establish the requirements for implementing and maintaining GRZ computer networks.

2.4.3 Guideline

1. All GRZ ICT networks shall be designed, configured and maintained according to the set GRZ minimum technical specifications and guidelines.

2. Only the GRZ ICT Units or their duly appointed delegate are to design, deploy and manage GRZ's ICT networks, and preserve their integrity in

collaboration with the nominated individual system owners (user departments).

3. No ICT hardware that does not belong to GRZ shall be installed on or connected to the GRZ network. The Responsible Officer for ICT may, however, formally approve usage of such equipment on restricted terms in special circumstances (i.e. consultants, students on short term engagements seeking to access the internet).

4. Security measures shall be put in place to protect data, voice, video and network infrastructure.

2.5 ICT Systems Operation and Administration

2.5.1 Overview

The administration and operation of an ICT system should be well structured. This can be achieved through the establishment of operation and administration procedures. This will help safeguard information and availability of the GRZ ICT systems.

2.5.2 Purpose

The purpose of this guide is to outline the requirements for administering and operating the GRZ ICT systems.

2.5.3 Guideline

1. GRZ ICT Hardware, other ICT equipment and information systems are to be managed by designated users from the ICT Units and user departments who are responsible for overseeing the day-to-day running of the systems.

2. GRZ's ICT Hardware, other ICT equipment and information systems shall be operated and administered using documented procedures by the ICT Units.

3. All ICT systems operation activities which include upgrades and any other that would impact on the availability of GRZ's ICT equipment and information systems are to be formally planned, authorised and documented by the responsible ICT section.

4. GRZ ICT equipment and information systems shall be used for GRZ's business purposes only, and this includes:

a) To facilitate performance of official duty, in a manner approved by Government procedures and guidelines; and

b) To acquire, provide and share information related to, or designed to facilitate the performance of duties.

5. Users of ICT Hardware and other equipment are solely responsible for the regular backup of GRZ information on their ICT equipment Appendix H Backup procedures.

6. Users of ICT systems shall only use legally obtained software from e-Government Division, which is suitably licensed on GRZ owned ICT equipment. Users shall be held liable for any breach of copyright.

7. All users of GRZ ICT systems and information systems have a duty to report all information security breaches or incidents on a timely basis so that prompt remedial action may be taken. As detailed in Appendix D Helpdesk Incident Ranking Scheme.

8. Users are expressly prohibited from the use of the GRZ ICT equipment and information systems for purposes that are not related to GRZ's legitimate activities and operations. These include among others:

a) Use of resources for private benefit such as the running of private business whether formal or informal; and

b) Transmission of material classified to be socially unfit for public and/or likely to cause disruption of services to others and compromise information systems security.

9. Users shall not intentionally run or operate any software that will damage, or otherwise hinder the performance of any ICT equipment or GRZ Business. Such software may be a virus or other malicious software.

10. GRZ employees, consultants, contractors, and any other third parties dealing with the MPSAs are not allowed to disclose non-public information accessed through the GRZ ICT systems to any unauthorised individuals. Necessary disciplinary action shall be undertaken in line with the conditions of service as detailed in Public Service Terms and Conditions of Service.

2.6 Disposing of Obsolete Equipment

2.6.1 Overview

ICT hardware and other equipment as assets do depreciate. After a period, this depreciation makes the hardware and other equipment either costly to maintain or simply obsolete and no longer useful. Such equipment may be disposed of at the MPSAs discretion. For example, the useful life of a Personal Computer (PC) is normally five years. After five years, various software upgrades would have been affected such that the operational efficiency and capacity of the PC may be rendered inadequate. Therefore, such a PC may be deemed obsolete and due for an upgrade, replacement or disposal.

2.6.2 Purpose

The guide is intended to address issues pertaining to disposing of ICT hardware and other equipment.

2.6.3 Guideline Statement(s)

1. A Personal Computer shall be used for five (5) years and after that it shall be due for an upgrade of components, replacement or disposal after a technical assessment of its performance by the ICT Unit. Appendix I Disposal of obsolete equipment – refer to GRZ Office Equipment Standard.

2. The ICT Units together with Stores Unit who are the custodians of the equipment shall recommend and supervise disposal of all ICT equipment and other hardware owned by GRZ in liaison with Ministry of Works and Supply. The responsible officers shall see to it that the disposal is carried out according to the laid down procedures. As detailed in GRZ Office Equipment Standards.

When disposing of the ICT equipment and other hardware the ICT Unit shall ensure that useful data is removed and secured appropriately.

2.7 Insurance of ICT Equipment

2.7.1 Overview

Insurance of ICT equipment and other hardware falls in the bigger picture of an organisation's business continuity strategy. In the case of loss of equipment to fire, theft or damage from disaster it is important that the hardware is quickly replaced for continuity of critical business applications. Insurance is one measure that can achieve this in good time and at low cost.

2.7.2 Purpose

This guide hereby establishes the insurance of ICT devices as a strategic requirement.

2.7.3 Guideline Statement(s)

It shall be the responsibility of the ICT Units together with the Purchasing and Supplies Unit to ensure that all critical ICT equipment and other hardware owned by GRZ are appropriately insured against theft, damage, or loss.

2.8 Equipment Relocation

2.8.1 Overview

GRZ has a national wide business network. This arrangement requires the movement of ICT equipment and other hardware between stations. Therefore, there is need to ensure adequate security and accountability in the process of moving equipment reference is made to Laid down GRZ procedures.

2.8.2 Purpose

This guide establishes how ICT asset transfer shall be carried out.

2.8.3 Guideline Statement(s)

1. When moving equipment from one office/station to another, the laid down GRZ general procedures and guidelines shall apply.

2. No equipment shall be moved without a dully approved Asset Transfer Form which could be manual or electronic. Appendix J Approved Asset Transfer Form – GRZ Office Equipment Standard.

3. GRZ officers will be allowed to move ICT equipment and other hardware from one office or station to another with permission from a responsible officer and supervision of ICT personnel.

CHAPTER 3

3 ACCESS CONTROL GUIDELINES

3.1 ACCESS AND PASSWORD

3.1.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of GRZ's entire corporate network. As such, all GRZ employees (including contractors and vendors with access to GRZ systems) are responsible for taking the appropriate steps in selecting and securing their passwords.

3.1.2 Purpose

The purpose of this guide is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.1.3 Guideline Statement(s)

The creation of passwords, their use and maintenance shall be in accordance with best practices and guidelines below and those listed in Appendix B.

1. Passwords for all administrative (access to all system functions) level accounts (e.g., root in UNIX system, Administrator in Windows and any other Operating Systems in use by the GRZ shall be changed on or at least within 60 days.

2. Administrative (access to all system functions) level accounts shall not be used for day-to-day activities. Administrators shall use their personal accounts, and request for added system privileges if necessary.

3. All administrative (access to all system functions) level passwords shall be stored in a secure place, and only be retrieved when needed. The responsible officer for ICT shall determine when to release these passwords.

4. If an account or password has been or is suspected to have been compromised the incident shall be reported to the Information Communication Technology Units within MPSAs and the password shall be changed immediately.

5. It is strongly recommended that GRZ user system accounts should not have the same password as that of a non-GRZ account (e.g., personal yahoo e-mail account, etc.)

even if both accounts belong to the same user. Where possible, different accounts for a single user shall have different passwords for various GRZ access needs.

6. GRZ account passwords shall not be shared, e.g., between administrative assistants and/or secretaries. All passwords are to be treated as sensitive, confidential GRZ information.

7. A user account that has been dormant for more than three months shall be deleted or locked and the owner of the account will have to request to have his/her account re-activated/ created. Communication from HRA to delete from the exchange server those who left the government.

3.2 Logon and Logoff Guideline

3.2.1 Overview

Information security demands that access to information is given to authorised individuals. Users requiring access to information must be verified for legitimate access. This is called authentication. Logon and logoff are security activities, which lead to verification (or authentication) of the request to access resources.

3.2.2 Purpose

This guide is intended to address unauthorised access to GRZ's ICT systems.

3.2.3 Guideline Statement(s)

1. Users shall strictly follow approved logon procedures as will be provided by the Information Communication Technology section. Appendix K Logon Procedure.

2. ICTs Units will train and assist Users not to leave their desktop/laptop screen unattended. Users shall either lock access to their computers or logoff.

3.2.4 Enforcement

Users of GRZ ICT equipment and systems shall enforce this guideline especially that unlawful access to their ICT equipment and systems shall be attributed to them as negligence which may lead to disciplinary action being taken under the staff disciplinary code.

3.3 Blank Screen Guideline

3.3.1 Overview

Confidential material can accidentally be exposed because information can be read from an unattended screen, especially when the computer/ laptop or any other ICT equipment with a screen is logged on and the owner is away from its location. A blank screen guide is an effective safeguard against this type of exposure of information.

3.3.2 Purpose

This guide is intended to address unauthorised access to GRZ's information via an unattended screen.

3.3.3 Guideline Statement(s)

All users of GRZ ICT equipment and other hardware, PCs and laptops are to ensure that their screens are clear/blank when not being used. One way to achieve this is to lock or logoff on the computer.

3.3.4 Enforcement

Users shall enforce this guideline especially that unlawful access to their ICT equipment shall be attributed to them as negligence which may lead to disciplinary action being taken under the staff disciplinary code.

3.4 Internal Communication and Collaboration

3.4.1 Overview

Information security demands that access to information is given to authorised persons. Users requiring access to information must be verified for legitimate access. This is called authentication. Logon and logoff are security activities, which lead to verification (or authentication) of the request to access resources. Users must ensure that organisational confidential information is not shared with un-authenticated users at any given time.

3.4.1 Purpose

This guide is intended to enhance the sharing of information to authorised individuals and the effective utilisation of shared services deployed in GRZ Institutions.

3.4.2 Guideline Statement(s)

1. Each User assumes responsibility for ensuring that GRZ information is not shared with un-authorised individuals.

2. GRZ does not guarantee the confidentiality of private information shared or stored on the Government Network.

3. For security and network purposes the ICT officers reserve the right to audit ICT systems and infrastructure.

4. Users are responsible to ensure that visitors who bring their own external storage are supervised at all times.

5. Whenever possible only connect to wireless networks that require a network security key and that information sent over these networks is encrypted to protect access to the Users machine.

3.4.3 Enforcement

Users of GRZ ICT systems shall enforce this guideline especially that unlawful access to their ICT systems shall be attributed to them as negligence which may lead to disciplinary action being taken under the staff disciplinary code.

CHAPTER 4

4 CONTROLLING INFORMATION SECURITY GUIDELINES

4.1 Confidentiality Agreements

4.1.1 Overview

Confidentiality is one of the security requirements in the use of ICT equipment and information systems. Confidentiality means that data should only be available to people it is intended for and that these people and/or any other person should not disclose it without due permission from the relevant authorities.

4.1.2 Purpose

The purpose of this guide is to outline and establish the requirements for managing confidentiality agreements for all users accessing public service ICT equipment and information systems.

4.1.3 Guideline Statement(s)

1. MPSAs, employees, consultants, contractors and any other third parties granted access to Public Service ICT systems shall sign a Government non-disclosure Agreement provided by the Government. Appendix L Government non-disclosure Agreement.

2. When a user or system administrator is accessing an ICT device which does not belong to him/her, for any reason, he/she shall not disclose, copy, distribute the information accessed except with permission from the owner of the information.

3. The User of the ICT equipment and Information System shall be required to uphold to the following core value statement defined by Cabinet Office, namely;

    a) Accountability
    b) Integrity
    c) Transparency
    d) Confidentiality
    e) Authorisation
    f) Authentication

4.1.4 Enforcement

This guideline shall be enforced when unlawful access is gained to GRZ equipment or information systems and may lead to disciplinary action in line with disciplinary code of conduct, regulation, GRZ Public Service Code of Conduct of conduct or any other legislation that may apply.

4.2 Internet Access

4.2.1 Overview

Government is mandated to provided Internet as a tool for availing resources to its employees to enhance their professional knowledge and hence improve productivity in the delivery of services. The Internet offers access to many valuable international, regional, national and local sources of information. However, some information found on the Internet may be inaccurate, incomplete, or offensive to some individuals. All MPSA employees must evaluate the validity and appropriateness of information.

4.2.2 Purpose

The purpose of this guide is to outline and establish the requirements and limits within which the Internet and intranet can be accessed using the GWAN.

4.2.3 Guideline Statement(s)

1. The following uses of the Internet shall be allowed but not limited to:

    a) To acquire information related to or designed to facilitate the performance of regular assigned duties.

    b) To facilitate performance of any task or project in a manner approved by Government.

    c) To facilitate for authorised information distribution to the stakeholders.

2. Users shall not use the Government Internet Services for the following purposes otherwise they are guilty of violating this guideline. The following uses are illegal and prohibited:

    a) Distribution of GRZ information to un-authorised persons or entities.

    b) Transmission of anything that causes disruption of services to others.

c) Intentional propagation of unsolicited material, and harmful software.

d) Possession, presentation, distribution and procuring of sexual, pornographic, or obscene materials.

e) Operating a business or soliciting money for personal gain.

f) Engaging in any activity in violation of International, National and/or Local Authorities laws.

g) Use of the Internet to have unauthorised access to any other computer and information system.

h) Downloading software packages for installation on GRZ ICT equipment by non-ICT staff. All downloads of software packages shall be done by the authorised systems Administrators in MPSAs and SMART Zambia Institute.

i) Obtaining both malicious software and any other inappropriate material.

3. Control mechanisms shall be put in place to ensure that internet resources are regulated to enable adequate utilization to enhance productivity in the effective delivery of service in the public service.

4.2.4 Enforcement

Employees, consultants and contractors who access the GWAN are responsible for making themselves aware of the legal consequences attached to the inappropriate use of those services.

GRZ ICT Users shall enforce this guideline especially that unlawful access to their ICT equipment shall be attributed to them as negligence which may lead to disciplinary action being taken under the staff disciplinary code or any other legislation that may apply.

4.3 Information Sharing (Intranet Access)

4.3.1 Overview

With the growth and prevalence of Internet usage, e-mail has become one of the most used forms of communication between MPSAs, employees, consultants, contractors, and any other third parties that have infrastructure capable for sharing resources.

4.3.2 Purpose

The purpose of this guide is to ensure that the information sharing tools provided by Government are used for the intended purpose.

4.3.3 Guideline Statement(s)

1. The following uses of information sharing tools such e-Mail, skype for business, SharePoint, teleconferencing IP Phones among others shall be adhered to:

    a) All Government employees are required to use official corporate mail or any other communication tools provided by e-Government Division

    b) Communication Tools provided by government must be used to communicate with Public Service employees, contractors, consultants and clients regarding matters relating to Government business.

    c) No abusive language shall be permitted in any manner when sharing official information in executing Government business.

2. Users shall be prohibited from using communication tools for the following purposes otherwise they are guilty of violating this guideline:

    a) Distribution of unsolicited non-Government business information or publications;

    b) Sending information using any Government communication tool without authorization from the supervisor;

    c) Transmission of any information that may cause disruption of Government services;

    d) Distribution or storage of pornographic or obscene material;

    e) Operating a business or soliciting money for personal gain;

    f) Engaging in any activity that violates any International, Regional, National and/or Local Authorities laws;

    g) Political Partisan related information; and

    h) Any other non-work-related information.

3. Users shall not open suspicious attachments and/or follow any suspicious downloads or instructions during information sharing, but instead report the matter to the head of ICT section.

4. All users shall take precaution when sharing information and shall ensure that the information is sent to desired recipients and for the intended purpose.

5. Only the Government ICT Units in MPSAs and Sever Management personnel are authorised to set up communication tools for all users in the public Services

6. The following considerations must be made in using official social media accounts;

   i. Be responsible in what one writes.
   ii. Remember to protect Government confidential information.
   iii. Respect copyrights.
   iv. Maintain Authenticity.
   v. Consider your audience.
   vi. Exercise good judgement.
   vii. Refrain from making views on behalf of GRZ.
   viii. Refer any communications on social media platforms to the responsible PR Unit.

4.4 Backup, Recovery and Archiving

4.4.1 Overview

Backup of the Government information files and the ability to recover such information is a priority for business continuity. In the case of ICT equipment and information system failure that results in the loss of information, backups can be used to restore the systems to their normal state. Therefore, the quality of the backups is cardinal since successful restoration depends on this. This guideline establishes the responsibility of conducting successful backups and restoration.

4.4.2 Purpose

The purpose of this guide is to outline and establish the requirements for backing up, recovering and archiving Government computer and information systems data and configurations.

4.4.3 Guideline Statement(s)

1. The GRZ ICT Units are responsible for ensuring that the frequency of backup operations and the procedures for backup, recovery and archiving meet the needs of the business.

2. Only the Government ICT Units or its duly authorised officers are mandated to backup, restore and archive critical Information Systems.

3. It is the responsibility of every user of Government ICT equipment to ensure that information and data stored on any ICT equipment is backed up regularly.

4. The Government ICT Section may assist with the responsibility for backing up for the users.

4.5 Systems and Equipment Update

4.5.1 Overview

These guidelines and procedures are set to guide GRZ Information Communication Technology Sections and general users on updating ICT equipment and system. These guidelines and procedures shall endeavor to be responsive to technological changes while remaining technological neutral.

4.5.2 Purpose

This guide relates to the establishment of the ICT Guidelines and Procedures on updating ICT equipment and systems, and the manner in which they are to be maintained and operationalised.

4.5.3 Guideline Statement(s)

1. The GRZ ICT Units are responsible for ensuring that the frequency of systems and equipment update operations and the procedures for updates meet the needs of the business.

2. Only the Government ICT Sections or its duly authorised officers are mandated to update critical Information Systems.

3. It is the responsibility of every user of Government ICT equipment to ensure that the ICT equipment is updated regularly.

CHAPTER 5

5 TECHNICAL SUPPORT AND SERVICE DESK MANAGEMENT GUIDELINE

5.1 Service Desk Management

5.1.1 Overview

System incidents are common in any organisation that heavily relies on ICT systems in doing business, especially large organisation like the Government. Therefore, measures should be put in place to ensure that system downtime is kept to the minimum as far as system failure resolution is concerned.

5.1.2 Purpose

The purpose of this guide is to establish how the ICT service desk related issues shall be managed.

5.1.3 Guideline Statement(s)

1. The Service desk team shall provide the ICT front office services. All computer operation incidents encountered by users shall be reported to the Service desk. Service desk personnel shall offer first level incident resolution. Occurrences of incidents beyond the MPSAs ICT staff jurisdiction or expertise shall be escalated to Service Management department under the e-Government Division.

2. Technical support shall be delivered on a first come – first serve basis and problems shall be resolved within the minimal time possible. All service requests for technical support are categorized in Appendix D Helpdesk Incident Ranking Scheme.

3. The contact and resolution times outlined in the Appendix D Shall be the ICT general guideline under normal operations.

4. All incident resolutions shall be recorded in the service manager system and documented by the ICT Service Desk personnel for future reference.

5.2 Contact details

The ICT Service Desk personnel can be contacted as listed below:

1. **Phone No:** (260-211) 253438, 254478
2. **Email:** info@szi.gov.zm
3. **Website:** www.szi.gov.zm

5.3 User Training

5.3.1 Overview

Applications that are deployed to carry out business functions are expected to deliver a given level of performance. However, it should be recognized that a good system might not be utilized to its fullest potential for lack of skills by the operators (e.g., users) and system administrators. It should, therefore, be a requirement that system users and system administrators have the right skills.

5.3.2 Purpose

The purpose of this guide is to establish procedures that will be followed to ensure that system users and system support have adequate skills to utilize computer applications developed or sourced outside GRZ.

5.3.3 Guideline Statement(s)

1. When implementing a new ICT system, users shall be trained on how to use the system before going live. The training shall be done by the ICT staff and the vendor where necessary for developed systems.

2. All applications shall be operated by trained and qualified users to avoid uncalled for down time, which might occur due to inappropriate use.

3. Technical training shall be offered to ICT staff for them to offer adequate support to systems. In the case of out-sourced systems, training shall be provided according to terms of any contractual agreements with outside suppliers.

4. GRZ users shall be provided with user manuals and formal training in using ICT systems.

5.4 Documenting Systems

5.4.1 Overview

System documentation is the development and management of well written information about a given system. This documentation may include user, technical, operational and development manuals. After development or enhancement, a system that has documentation is easier to maintain than one which does not have. Thus, the need to have system documentation.

5.4.2 Purpose

The purpose of this guide is to ensure that information systems are adequately documented.

5.4.3 Guideline Statement (s)

1. All information systems shall be fully supported at all times by comprehensive and up to date documentation.

2. New or upgraded information systems should be introduced to a working environment with the necessary documentation to support maintenance of the same.

4. Changes to the operation of information systems should be documented with appropriate circulation of information on the change to all concerned users.

5. Provision of documentation for outsourced systems shall be the responsibility of the vendor. All in-house developed systems documentation shall be the responsibility of the systems developers.

5.5 Disposing of Software

5.5.1 Overview

Software is often desirably licensed indefinitely. However, a change of business circumstances or other external factors (such as change in legislation) may result in a decision to stop using a certain system or to move to another.

5.5.2 Purpose

This guideline ensures that the correct safeguards are put in place in disposing of business software that is no longer required by GRZ.

5.5.3 Guideline Statement(s)

1. The disposal of customized software shall only take place after approval by the ICT section that the system is no longer required and that its associated data files which may have been archived will not require restoration at a future point in time.

2. The disposal of shared software shall be done under e-Government Division.

3. Data retention in each institution must adhere to the relevant legal and regulatory framework as provided for in the respective sector.

5.6 Signing for Work Done by Third Parties

5.6.1 Overview

After an IT project is completed by a third party, a signature, usually from a project manager or system owner, is required to verify that the work done is complete. This is part of the Change Control process and also forms part of the audit trail. A signature by a technical person from the Information Communication Technology is mandatory for quality control purposes.

5.6.2 Purpose

The purpose of this guide is to ensure that all work carried out by third parties is properly done according to the agreed requirements.

5.6.3 Guideline Statement(s)

Upon completion of a project by a third party, the project manager or the system owner in conjunction with the responsible ICT officer shall accept the work done by way of a signature. Only authorised persons are permitted to sign for work completed

5.7 Bring Your Own Device (BYOD)

Bring your own device (BYOD) is no longer simply a catch phrase or a new trend, it's reality. It entails that many employees use their own devices to access corporate assets such as network drives, documents, printers, web proxies, social media sites, and personal cloud services. Malware, viruses, theft, unsecured devices, jailbroken devices, and a lack of control on employee owned devices puts corporate data, intellectual property, and client information at risk. To manage this problem MPSAs shall enforce BYOD guidelines to secure information systems and information in the work environment.

These BYOD guidelines provide the first step in curbing the possible chaos that could be brought about through the use of personal devices for official business. If users want to conduct official business via the use of their own devices, they must follow these guidelines.

Since security is an ongoing process that requires vigilance, administration, revision and flexibility, the BYOD guidelines below, if enforced with the help of security standards, shall enable all MPSAs to safeguard sensitive data:

5.7.1 Jailbroken and rooted devices are not allowed.

Most, if not all, mobile security suites consider jailbroken (i.e. devices on which all imposed iOS restriction have been removed) and rooted devices to be "security compromised." These compromised devices are exposed to security vulnerabilities, malware, viruses, and hacks that secured devices are not.

5.7.2 Devices must be protected by screen lock passwords

MPSAs guidelines shall require data protection practices to be put in place, including requiring strong passwords, automatic locking after periods of inactivity, establishing protocols for reporting lost or stolen devices, mandating certain antivirus and protective software, and requiring or strongly encouraging regular backups. Mobile security suites can enforce the use of a screen lock password on any user device.

5.7.3 Require enrolment in the corporate Mobile Security Management Suite

To enforce security policies at the device, application, or document level, MPSAs use a mobile security management suite. The suite should integrate into your environment such that no user device may access corporate assets without first enrolling in and being vetted by the security policies. To bypass enrolment puts other users and their devices at risk.

5.7.4 Devices must be regularly updated with latest Operating System and patches

To stay ahead of malware, MPSAs shall keep their devices updated to the latest operating systems. This updating includes minor updates that may fix security vulnerabilities between major revisions. MPSAs can enforce update policies and push updates from some mobile security management suites to ensure that user's devices maintain the highest available patch levels. Consider keeping a registry of all personal devices being used for business purposes.

5.7.5 Business data and personal data must be kept separate

Management suites have the capability of wiping data from devices, MPSAs shall provide a set of apps that hold their own data separate from user data. This separation is achieved through good app planning and programming and management suite policy enforcement. The separation will facilitate security measures the employer wishes to impose on their personal data and will limit employer access to work data only. Clearly state the employer's right to access, monitor and delete information from employee- owned devices. If the MPSA is allowed to access personal information, state the circumstances under which it might do so.

5.7.6 Corporate data should be encrypted

All data within, or accessed by, MPSAs (Corporate apps) should be encrypted so that compromised devices don't give up their data in readable form. If users can access data in offline mode, app data is especially sensitive and must be encrypted to ensure security.

5.7.7 Custom profiles for each device type and manufacturer

Employees in MPSAs might bring a variety of device types (tablets, phones, laptops) and manufacturers to the workplace. A separate security should be available for each supported device specific to that device. Generic security guidelines will leave significant gaps and create additional vulnerabilities on your network. Most mobile management suites support a variety of device types and manufacturers Devices outside of the support matrix should not be allowed as part of the BYOD program.

5.7.8 Require Virtual Private Network (Application or Device) for connectivity

To ensure that all communications with the corporate network are secure Virtual Private Network (VPN) connection enforcement should be standard. Device-level VPNs securely connect the entire device to the corporate VPN server, whereas application- level or micro VPN connectivity ensures that all application-related data transmissions are secure.

5.7.9 Require periodic re-authentication

Periodic re-authentication assures that the user is genuine. Unlimited access without reauthentication is a security vulnerability for any device that might be stolen or compromised during authenticated use. Management suites can enforce reauthentication after a set time period.

5.7.10 Prevent offline access

MPSAs require a very high level of security for documents or applications therefore, they must prevent any offline access to them. MPSAs must not allow documents or data to be downloaded or cached on the local device. MPSAs shall allow access to sensitive information while connected to the GWAN.

5.7.11 Harmonise MPSA Policies and Protocols

Revise current MPSA policies and protocols that may be affected by BYOD practices. This may include adjusting record-retention policies to cover data on employee-owned devices. Revisit data breach protocols to ensure that they cover situations where sensitive data (such as Social Security numbers and credit card information) is compromised. Designate who is responsible for authorizing work-related software and other downloads, as well as a main point of contact for questions about the policy. It is also recommended to post a resource page or frequently-asked-questions page on your organisation's intranet.

Provide reasonable notice to employees as to when employer data will be "wiped" from personal devices. The organisation should determine whether all data (personal and work) will be deleted or just work information and how the company will make the distinction between work and personal information. It should be addressed whether employees will be afforded the opportunity to review the data being removed or to preserve personal files and in which instances will employees be asked to surrender their personal devices for inspection and removal of employer records (for example, investigations, IT servicing or termination of employment).

MPSA policies should also define which classes of employees will be permitted to use their own devices and why. Employees will be required to agree with acceptable-use terms when they first connect with the employer's computer network.

It should also be communicated whether the MPSA will introduce any new forms of monitoring, such as location-based tracking via GPS or other methods on employee owned devices. If so, specify when the monitoring will be used by the employer and for what purpose.

APPENDICES

A) Password guidelines

General Password Construction Guidelines

Poor, weak passwords have the following characteristics:

1. The password contains less than eight characters.
2. The password is a word found in a dictionary (English or foreign).
3. The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names such as for commands, sites, hardware components, software tools, etc.
    - The words 'GRZ', 'Lusaka', 'Chipata' or any derivation.
    - Birthday and other personal information such as address and phone number.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

1. Contain both upper- and lower-case characters (e.g., a-z, A-Z).
2. Have digits and punctuation characters as well as letters e.g., 0-9, !@()^%& +|-=[]:;?,./).
3. Are at least eight alphanumeric characters long.

4. Is not a word in any language, slang, dialect, jargon, etc.

5. Are not based on personal information, names of family, etc.

6. Are based on a song title, affirmation, or other phrase. For example, the phrase might be: 'This May Be One Way to Remember' and the password could be: 'TmB1w2R!' or 'Tmb1W%r' or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection guidelines

Here is a list of don'ts:

1. Don't reveal a password over the phone to ANYONE.
2. Don't reveal a password to your boss.
3. Don't talk about a password in front of others.
4. Don't hint at the format of a password (e.g., 'my family name').
5. Don't reveal a password on questionnaires or security forms.
6. Don't share a password with family members.
7. Don't reveal or insert passwords into email messages or other forms of electronic communication.
8. Don't reveal a password to co-workers while on vacation.
9. Don't give anyone a password even if they demand for it, but refer them to this document or let them call someone from the Information Communication Technology Sections.
10. Don't use the 'Remember Password' feature of applications (e.g., Eudora, Outlook and Netscape Messenger).
11. Don't write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

B) Software Acquisition

Software Acquisition Approval

The following are the guidelines, which shall be followed to initiate the process of acquiring a new system.

1. User(s) shall request for a new system (i.e., by presenting the request to their head of department).

2. The Head of Department will either approve or reject the request.

3. If approved, the request shall be submitted to the Procurement Specialist.

4. Once approved, other activities will follow as stipulated in the technical ICT Procedures Manual.

C) Helpdesk Incident Ranking Scheme

Priority Issue Contact Resolution

Priority	Issue	Contact	Resolution
1	Issue of the highest importance such as failure of a critical or essential system e.g. GRZ Information Systems, FMS	5 minutes	30 minutes
2	Single user or group outage that is preventing the affected user(s) from working. e.g., failed hard drive, broken monitor, continuous operating system lockups, etc.	15 minutes	1 Hour
3	Single user or group outage that cannot be permanently or temporarily solved with a workaround. e.g., malfunction printer, PDA synchronization problem, PC sound problem, etc.	30 minutes	1 day
4	Scheduled work. e.g., new hardware or software installation, etc.	1 Hour	1-4 Days
5	Nonessential scheduled work. e.g., office relocation, telephone moves, equipment loaners, etc.	1 Day	5 Days

Table C.1: Incident Ranking Scheme with contact and resolution time

D) Government Minimum Technical Specifications Guidelines – Refer to ICT Minimum Specifications

E) ICT Communication Systems Configuration and Maintenance Guidelines – Refer to Acceptable Use Guidelines

F) GRZ ICT Security Specifications – Refer to Public Service Information Security Standard

G) Backup Procedures

The following are the guidelines, which shall be followed when carrying out a backup.

1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner. The Organisation Information Resources backup and recovery process for each system must be documented and periodically reviewed.

2. The vendor(s) providing offsite backup storage for the Organisation must be cleared to handle the highest level of information stored.

3. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest Organisation sensitivity level of information stored.

4. A process must be implemented to verify the success of the Organisation electronic information backup.

5. Backups must be periodically tested to ensure that they are recoverable. This period shall be set according to the criticality of the data backed up and the frequency of its change Signature cards held by the offsite backup storage vendor(s) for access to Organisation backup media must be reviewed annually or when an authorised individual leaves Organisation.

7. Backup tapes must have, at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:

i. System name
ii. Creation Date
iii. Sensitivity Classification [Based on applicable electronic record retention regulations.] and
iv. Organisation Contact Information

All user information on the servers must be identified and scheduled for back-up in line with the routine back up procedures based on the sensitivity classification.

H) Disposal of Obsolete Equipment – Refer to GRZ Office Equipment Standard

I) Asset Transfer Form – Refer to GRZ Office Equipment Standard

J) Logon Procedures – Refer to Acceptable Use Guidelines and Procedures