NITA UGANDA

- Driving the IT Revolution -

Guidelines for Operation, Usage and Management of Information Technology Infrastructure in MDAs & Local Government

Version Number:	**1.0**
Date:	**September 2013**

DOCUMENT DETAILS

Security Classification	Government/Public		
Authority	National Information Technology Authority-Uganda (NITA-U)		
Author	National Information Technology Authority-Uganda (NITA-U)		
Documentation Status	**Working Draft** √	**Consultation Release** ☐	**Final Version** ☐

CONTACT FOR ENQUIRIES AND PROPOSED CHANGES

All enquiries regarding this document should be directed to the Office of the Executive Director.

info@nita.go.ug

ACKNOWLEDGEMENT

This version of the guidelines and standards was developed and updated by the Department of Architecture, Standards and Certification under the Directorate of Planning Research and Development, National Information Technology Authority-Uganda (NITA-U).

Feedback was received from a number of staff from the other Directorates which was greatly appreciated.

Foreword

The National Information Technology Authority-Uganda a semi-autonomous corporate body established under the NITA-U Act 2009, to coordinate, promote and monitor IT development within the context of National Social and Economic development.

The Authority is financed in part by parliamentary appropriation. The NITA-U policies and operations are managed at arm's length from Government. NITA-U is overseen by a Board of Directors whose membership includes government and private-sector representation.

With the goal of enhancing Uganda's economic competitiveness and social well-being, NITA-U leads the efforts of Ugandans in the development and use of national and international IT standards and further intends to offer a range of IT standardization services to the citizens of Uganda. One such service in line with the NITA-U mandate is the integration of all Government IT systems in line with the strategy for rationalization of IT services in Government Ministries Department and agencies

It is important that IT services are offered with the highest standards, in the most comprehensive way and with the best possible IT products to meet user expectation.

This document therefore provides general guidance in the operation, management, usage and maintenance of IT infrastructure implemented across Government Ministries, Department and Agencies including local Governments to ensure availability and integrity of the infrastructure.

The NITA-U within its mandate shall continue to provide technical guidance in line with the operation, management and usage of all Government IT systems for efficient delivery of IT services across Government MDAs/LGs and local Governments.

EXECUTIVE DIRECTOR

TABLE OF CONTENTS

List of Acronyms

ER : Equipment Room

ICT : Information and Communications Technology

IT : Information Technology

LG : Local Government

MDA : Ministries, Department and Agencies

NITA-U: National Information Technology Authority-Uganda

PCs : Personal Computers

PDAs : Personal Digital Assistants

PDF : Portable Document Format

PPDA: Public Procurement and Disposal of Public Asset Authority

TR : Telecommunications Room

SLA : Service Level Agreement

SPAM: Self-Propelled Automatic Mail

TO : Telecommunications Outlet

UNBS: Uganda National Bureau of Standards

UPS : Uninterrupted Power Supply

List of figures

List of Tables

1. INTRODUCTION

This document is developed to guide government Ministries, Departments, Agencies (MDAs/LGs)/Local Government in adoption of common standards in order to promote good practices in the Government-wide use of Information Technology (IT).

This document presumes the reader has some familiarity with basic IT and Internet terminology, development and design. It summarizes key aspects of IT issues and is intended to act as a ready reference guide.

This document has four (5) main sections:

1. Operation of IT equipment
2. Management and Usage of IT Infrastructure
3. IT Equipment and Software Management Guidelines
4. Maintenance and Repair of IT equipment
5. Human Capacity development

The use of these guidelines shall help to ensure that the use of IT infrastructure across government in the delivery of IT services is done to a consistently high standard. This shall lead to increased confidence and rapid uptake in the use of IT and the Internet within Government as well as increased customer satisfaction in government services delivery.

As stipulated in the NITA-U Act 2009; Objects of Authority; Section 4(b); one of the core objective of NITA-U is "To promote standardization in the planning, acquisition, implementation, delivery, support and maintenance of information technology equipment and services, to ensure uniformity in quality, adequacy and reliability of information technology usage throughout Uganda"

1.1 Objectives of the Standards

The main objective of these Standards is to provide best practice guidelines for use in the operation, usage, management, maintenance and repair of IT equipment in MDAs/LGs.

1.1.1 Specific Objectives

The specific Objectives shall be:

1. To facilitate proper usage and operation of IT equipment to extend their useful life

2. To enhance capacity to support and maintain IT equipment in MDAs/LGs and Local Governments

3. To provide efficient and cost effective means of implementing and managing IT equipment in MDAs/LGs

4. To ensure that IT equipment are securely managed in the Government MDAs/LGs and local Government

1.2 Applicability

These set of guidelines shall be applicable to Government MDAs and Local Governments and may in addition be useful to Institutions outside Government settings such as the private sector organization Academia etc. The guidelines stipulated in this document provides best practices for appropriate management, operation, usage and maintenance of IT infrastructure by IT personnel, end-users and Administrators in those Institutions. It is intended to be applied along-side other established IT Policies within the respective MDAs.

2. OPERATION OF IT EQUIPMENT

It is important that MDAs/LGs observe these guidelines for operating IT equipment to ensure maximum utilization in a manageable and sustainable manner. Improper handling and operation of equipment leads to failure before their end of life.

2.1 Guidelines for operating IT equipment

1. The IT Units within the respective MDAs/LGs shall ensure that configurations of the components of the network or system shall be documented for the purpose of maintenance and future planning.

2. Only staffs within the respective MDAs/LGs are authorized to use IT equipment and software resources. Any other person will be required to seek approval from IT Unit for use of IT equipment and resources.

3. MDA should encourage staff to be considerate in their use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.

4. All MDAs/LGs shall ensure that there is sufficient warranty on all IT equipment and software in use

5. The IT Unit in each MDA shall ensure that entry to the Server Room shall remain restricted to IT Unit staff.

6. All Data pertaining to the MDA shall be stored on appropriate Backup Media

2.2 User Responsibilities

In making acceptable use of IT resources users must:

1. Use IT resources only for authorized purposes

2. Scan any external disk (CD, flash disk, hard disk etc.) with Antivirus before using the same on the network/desktop; this will minimize the risk of virus infection.

3. New users should obtain official e-mail addresses from the IT Unit/department

4. Use only legal versions of copyrighted software in compliance with vendor license requirements.

5. Print only what should be printed noting that Information can still be useful in electronic form.

6. Shred any printed sheets before throwing them into the bins. No sheets bearing MDAs/LGs data should be discarded without being destroyed.

7. Ensure that requisite approval is sought before Diskettes/ flash disks containing MDAs/LGs data are released to any other external party.

In making acceptable use and operation of IT resources users MUST NOT:

1. Use computer programs to decode passwords or access control information.

2. Attempt to circumvent or subvert system or network security measures

3. Use another person's system, files, or data without permission (note that permission from an individual user may not be sufficient - some systems may require additional authority).

4. Give passwords to others, without due consideration. It is necessary to contact IT Unit if one needs access to information, which they are not automatically authorized to access

5. Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, worms, or "Trojan horse" programs; disrupting services; damaging files; or making unauthorized modifications to corporate data.

6. Waste shared computing or network resources, for example, by printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings

2.3 Information/Data Security

Due to the importance of data in any given enterprise, the IT Unit shall take regular backups and any other security measures to ensure that the MDAs/LGs data is safe and can be relied upon in the event of online data loss.

The following security measures shall be taken to safeguard MDAs/LGs data: -

1. The IT Unit will keep proper backup of all data in the MDAs/LGs.

2. The data backup will be on daily basis and retained for a period approved by Management. All backups shall be securely kept and protected from any damage or data loss

3. Due to the frequent change in technology, the backup media shall be revised consistently to ensure that all the backups are accessible and can be redeployed when needed.

4. The Backup Media shall be kept in the designated secure and safe place appropriately.

5. The backups of computer systems shall be kept in safe internal and external areas to eliminate any chances of damage in the event of disaster.

6. Backup procedures shall be revised from time to time to ensure compliance with the current security trends

2.4 Information Backup Guidelines

The following shall be considered in backing up of MDAs/LGs Information:

1. MDAs/LGs shall ensure accurate and full records of the back-up copies and documented procedures for restoration should be developed;

2. Backup shall be done on a daily basis, for system states and data on all the servers.

3. Back-ups shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster such as fires, floods or earthquakes from the main site;

4. MDAs/LGs shall ensure that back-up media are regularly tested to ensure that they can be relied upon for emergency use when necessary;

5. MDAs/LGs shall ensure that backup is protected by appropriate procedures such as encryption.

2.5 IT equipment Electrical safety

1. All electrical equipment should be maintained regularly. Always leave technical repairs to the experts.

2. Ensure that to have the necessary fire extinguishers positioned near any IT equipment room.

3. The location of IT equipment depends on the length of cables and the availability of sockets for telephones, data and power. It is essential that the location of the equipment does not increase the risk of danger to equipment or users.

4. Particular issues to be aware of are as follows:
   (a) Cover and secure trailing power cables.
   (b) Replace worn out leads or damaged plugs.
   (c) Do not overload circuits, particularly when using long extension leads, as power surging can occur if much IT equipment is connected to a circuit, or when electrical floor cleaning equipment is plugged in.
   (d) Avoid coiled cables, as the heat generated within them could be sufficient to start a fire.
   (e) Be aware of accidental damage, particularly any cuts to power cable insulation, and also damage from dust, spilt liquid.
   (f) Ensure that the correct fuse rating is fitted to the IT equipment

5. IT personnel shall ensure that connecting cables (to keyboards, mouse etc.) do not hang over the front of the computer workstation.

6. Trailing loops of cable at the rear of machines should be tidied to allow easy access to equipment for maintenance and to prevent equipment from being dragged accidentally from the workstation.

7. It is important to ensure that procedures are put in place for regular visual checks of plugs, leads & other electrical equipment for safety etc.

3. MANAGEMENT AND USAGE OF IT INFRASTRUCTURE

This section provides the fundamental set of principles for the proper usage of the IT Infrastructure installed in the different MDAs/LGs.

The guidelines laid down below governs the terms and conditions for the use of the services that are offered within the IT infrastructure installed within the MDAs as well as the respective Local Government headquarters.

It obliges the user to act in an appropriate manner and to use the provided IT resources in an economical way as well as to operate the system correctly.

3.1 Application for Admission to use the IT Infrastructure

The application for admission to use the IT infrastructure in the different MDAs/LGs shall contain the following information:

1. The Particulars of the Designated IT personnel who receives the application for admission;

2. The IT infrastructure/system (s) for which admission is requested;
3. Description of the intended use of the IT equipment and/or the planned activities(e.g. research, teaching, storage and issue of information, administration and work related);

4. Statement of acceptance made by the applicant that he or she accepts the policy of use of the IT equipment and other related resources.

5. Warning that the applicant's user activities may be recorded on the basis of the Policy in use.

3.2 Admission to use the IT Infrastructure

It is important for IT personnel in the respective MDAs/LGs to ensure that mechanisms (such as procedures to use and IT equipment) are put in place to allow staff use IT equipment.

1. To use the IT resources installed within the MDAs/LGs; the user must have a formal authorization issued by the responsible Network or System Administrator or any other designated IT personnel (e.g. a user ID, network connection or network access authorized by the Network/System Administrator)

2. The use of computerized services (e.g. details of e-mail addresses, internet access, extensive computing time or storage capacity, use of computer tools) are governed by the policy of use issued by each respective MDAs/LGs.

3. Computers and other related IT equipment that are operated by non-members of staff within the respective MDAs/LGs may not be connected to the network unless this has been authorized on the basis of special provisions and in cooperation with the Network Administrator.

3.3 Rejection/Withdrawal of Admission to use the IT infrastructure

Admission to use of IT equipment and resources may be rejected, withdrawn or limited in part or as a whole, in particular when:

1. No acceptable application has been submitted or when the information given in the application is incorrect or obsolete;

2. The applicant's intended activities are incompatible with the tasks for which the IT equipment or system has been installed to accomplish;

3. The current levels of use of IT equipment or resources exceed the capacities required for the intended use;

4. The purpose of use of the IT infrastructure will potentially impair the functionality of authorized IT systems in an unacceptable way;

3.4 Guidelines for Usage of IT Infrastructure

Upon admission to use the IT Infrastructure in the respective MDAs/LGs; staff shall be required to observe the following guidelines;

1. The users are entitled to use the IT Infrastructure as approved and as permitted by the policy in their respective MDAs/LGs. Any usage other than permitted by these regulations and policies requires special approval;

2. The users must comply with the provisions of these guidelines and act within the boundaries of their admission and observe the following:

   (a) Users are required to refrain from all activities that will disrupt proper operation of the IT Infrastructure in the respective MDAs/LGs

   (b) They are required to handle all data processing systems, information and communication systems, as well as other resources of the IT Infrastructure with due care; to use only the IT equipment accorded to them as permitted.

   (c) To take due care that their user passwords and user IDs are not made known to others and to make sure that these IT equipment are not accessed by unauthorized

individuals; this includes the protection of the access with a strong password (difficult to guess) that must be kept confidential and should be changed on a regular basis;

(d) Not to gain knowledge of or make use of other individual's user IDs/passwords;

(e) Not to access information, and in particular, not to access other individual's messages/information (E-mails etc.) without their authorization and not to pass on, use or modify any information gained without their approval;

(f) When using software (sources, objects), documentation material and other data, the user must adhere to the legal provisions (e.g. copyrights) and must comply with the contractual provisions (e.g. license agreements) under which the software was purchased.

(g) MDAs/LGs shall ensure that software are not copied and passed to third parties or to use them for purposes other than those permitted explicit permission has been granted by the relevant authorities.

(h) Not to correct, mend or rectify problems, damage and errors on any IT Infrastructure or resources and data media but to immediately report them to the responsible Network/System Administrator or any other designated IT Personnel within the respective MDAs/LGs;

(i) Not to make changes to hardware installations and/or to the configuration of the operating systems, system files, and user files that are required by the system, and to the network, unless explicit approval has been obtained;

3.5 Exclusion from Use of the IT Infrastructure

Exclusion of MDAs/LGs staff from the use of IT Infrastructure shall be on the following grounds:

1. Users may temporarily or permanently be limited in or excluded from the use of the IT Infrastructure or resources;

(a) If they intentionally or negligently violate these guidelines and, in particular carrying out abusive actions (such as illegal and other acts motivated by racism, racial discrimination and related intolerance, hatred, violence, all forms of child abuse, including child pornography, and trafficking, and exploitation) on the IT Systems.

(b) When they abuse the use of IT Infrastructure and resources for illegal/criminal acts such as fraud and authorized use interception of data or information traversing the network etc.

(c) When they cause harm to the Government MDAs/LGs by unlawful user behavior

2. Temporary usage restrictions that will be implemented by the responsible Network/System Administrator have to be lifted as soon as compliant use can be expected.

3. A permanent restriction or revocation of user rights is only possible in cases of severe and repeated violations and when compliance cannot be expected in the future, although actions have already been taken. The decision to permanently remove the privileges to use an IT Infrastructure system shall be made by Administrative notice upon application by the Network/system Administrator.

3.6 Responsibilities of the IT Personnel

The following shall be the responsibilities of IT Personnel across all MDAs/LGs:

1. Each designated IT personnel in the respective Government MDA/LGs shall inform users on the usage, important facts and the relevant rules and regulations to be complied with, and in particular, on their privileges and responsibilities.

2. IT personnel within the MDAs/LGs shall maintain a user file containing the personal data of the users. A summary of the type of data stored must be accessible to each user at any time.

3. IT personnel shall limit or block the use of IT Infrastructure or resources for purposes of troubleshooting, system administration and system extension, system security implementation as well as for maintenance. All the affected users have to be informed ahead of time.

4. IT personnel shall protect IT infrastructure and user data from unauthorized access by third parties. IT personnel may apply manual or automated check procedures on a regular basis to control the security of the systems.

5. IT personnel shall ensure that user passwords are changed on a regular basis. Changes made on user passwords, access privileges to user files and other user-relevant protective measures have to be communicated to the users appropriately.

6. IT personnel shall periodically document and evaluate how individual users use the IT infrastructure for the following reasons:

   (a) To ensure correct operation of the IT Infrastructure and systems put in place.

   (b) To plan resources and to administer the system.

(c) To determine the user patterns of the installed IT infrastructure

(d) To protect the personal data of other users

(e) For billing purposes

(f) To identify and correct system malfunction;

(g) To detect and prevent abusive, or unlawful use

7. IT personnel shall access user files deemed to be the source of malicious attack or abuse of MDAs/LGs computer system. This access shall be implemented in the presence of an administrator/staff authorized by the accounting officer and the process documented.

   The affected user has to be notified immediately when the purpose for access of his/her user files have been attained. If the investigation provides evidence for punishable offences/criminal act, the IT personnel shall report the incident to the Accounting Officer in those particular MDAs/LGs.

8. IT personnel shall ensure that staffs do not store contents on computer systems that violate the MDAs/LGs IT Policy or the provisions contained in this guidelines. Ensure to put in place measures to block and seize such illegal content.

9. To ensure proper operation of the IT system, each IT personnel is required to check the e-mail traffic for malicious programs (e.g. virus, unsolicited bulk e-mail or SPAM) using automated procedure. If the investigation provides actual evidence that an e-mail contains a malicious program it must be automatically deleted;

10. IT personnel shall not communicate personal data or operating data, connection data and user data that enable the identification of individuals to third parties

3.7 User liability

Users of the all installed IT infrastructure shall be liable in case of the following:

1. Users shall be held liable for all hindrances incurred to the MDAs/LGs as a result of wrongful or illegal use of the IT Infrastructure, resources, user admission or that which arises as a result of the user's intentional or negligent violation of these guidelines.

2. The user shall also be held liable for damages caused by third parties, if the user is accountable for third parties using his or her access and user privileges; this applies in particular to third parties using his or her user ID.

3. MDAs/LGs may claim compensation for the wrongful use of IT resources and other costs which have to be borne by the user such as damage caused on an IT asset.

3.7.1 Sustainable Use of IT Equipment

The following sustainable use of IT infrastructure shall be adhered to by all MDAs/LGs

1. MDAs/LGs shall ensure that users are trained to turn on and off any IT equipment for use and after use. Note that leaving non-critical computers powered on when not in use consumes powers.

2. A screen saver message reminding staff to turn IT equipment off when not in use should be implemented

3. MDAs/LGs shall ensure that staffs are trained to turn off monitors, printers, scanners and other IT equipment at night or after office hours.

4. Encourage the use of conferencing technologies (audio and video) for staff training and meetings, to reduce the need for travel

5. MDAs/LGs shall ensure centralized multi-function networked printing and scanning devices, deployed based on a workflow requirement are installed. Avoid proliferation of desktop peripherals such as printers, scanners and fax machines.

3.8 Password Management

Passwords are front line protection for user accounts and are important aspect of computer security. A poorly chosen password may result in the compromise of the MDAs/LGs entire network. All staffs are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purposes of these guidelines are to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All system users must observe the following password guidelines:

1. All system-level passwords (e.g. root, Administrator, admin, application administration accounts, etc.) must be changed regularly or whenever need arises.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every after (one) months.

3. User accounts that have system-level privileges granted through group memberships such as financial systems must have a unique password from all other accounts held by that user.
4. Passwords must not be inserted into email messages or other forms of electronic communication.
5. Passwords should not be written in note books for reference.
6. Password should not be shared
7. Report to the IT unit if you have forgotten your password

Some of the more common uses of passwords include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

3.8.1 Poor and weak passwords characteristics

The following are some of the characteristics of weak passwords which the IT personnel in MDAs/LGs should encourage their staff to avoid:

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:
    (a) Names of family, pets, friends, co-workers etc.
    (b) Computer terms and names, commands, sites, companies, hardware, software.
    (c) Birthdays and other personal information such as addresses and phone numbers.
    (d) Word or number patterns like aaabbb, 12345, etc.

3.8.2 Strong passwords features

IT personnel shall encourage the use of strong passwords with the following characteristics:

(a) Use both upper and lower case characters (e.g., a-z, A-Z)
(b) Have digits and punctuation characters as well as letters e.g., 0-9,
(c) !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
(d) At least eight alphanumeric characters long
(e) Words not in any language, slang, dialect, jargon, etc.
(f) Avoid personal information, names of family, your car name etc.

(g) Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.

4. WEBSITE MANAGEMENT AND UASGE

The Internet is becoming a preferred means of accessing government information and services. Therefore, a crucial element of an effective web presence is quality and relevance of information posted on Government websites.

Government MDAs/LGs shall develop websites that contain informative and up-to-date content that is well-written, caters for the needs of a wide range of audiences and is easily accessible. MDAs/LGs must therefore ensure that:

1. Information provided on website meets the needs of consumers
2. Information provided is current
3. There is a consistent approach across websites
4. At least a minimum set of information is provided

Information presented on a government website must be consistent with government policies to avoid the possibility of damage to both the government and consumers if information is incorrect or inappropriate.

4.1 Posting Information on MDA Websites

It is recommended that government MDAs/LGs include publications that are available to the public through other forms of media (such as hardcopy or audio) on their websites. The same shall be captured linked in the online library. Where this is not practicable due to, for instance, high costs, limited benefits, low demand, publication complexity information on how to obtain a copy in its original form should be posted on the website. Any decision not to publish in electronic form rests with the Accounting Officer.

4.2 Information Request and Feedback

MDAs/LGs are required to provide full contact details, including physical service locations, fax and telephone numbers, and mailing addresses. Email addresses shall also be provided, in particular, for the entity responsible for maintaining the website for the purpose of reporting fault. A general enquiry email address for the MDAs/LGs shall be established so as to protect the

individual name and person, which consumers can contact in relation to the MDA/LGs service offerings.

4.3 Legislative and Sector Information

Policy documents, legislative and sectoral information related to the MDAs/LGs shall be provided on their website. This information shall not be duplicated on any other MDAs/LGs websites, instead links shall be provided to relevant resources at the various source websites. These include, but not limited to:

(a) The Constitution of Uganda

(b) Legislation and legislative status information

(c) Bills and Acts

(d) Sectoral policy documents

(e) Circulars, Policy Documents, Publications and Reports among others.

4.3 On-line/Electronic Forms

There are several types of forms that can be used to present and collect information from users; Interactive forms, e-forms and downloadable forms.

1. MDAs/LGs shall ensure that for interactive forms, appropriate security precautions shall be put in place to safeguard user information during transmission and storage. MDAs/LGs shall also ensure that user input errors are minimized by helping users identify, avoid and correct mistakes.

2. MDAs/LGs shall ensure that e-forms and downloadable forms are in compatible formats and where special software is required, a link to download it must be provided. For these types of forms, pdf format is recommended.

3. Government MDAs/LGs shall continuously endeavor to provide online interactive forms, and where not possible, a downloadable format shall be made available.

4.4 Information not permitted on MDAs/LGs Websites

The following guidelines shall be provided:

1. Government websites shall not post information that does not promote the MDAs/LGs Government policy. In addition, the following content shall not be permitted:

(a) Commercial banner advertisements
(b) Personal information
(c) Politically partisan content

2. Government websites can however acknowledge sponsors and partners at a section on their website but this decision rests with the appropriate senior executive within the MDAs/LGs, provided it is consistent with government policy.

3. Banners that promote and link to other government MDAs/LGs are permissible, provided that no fees are charged in placing such banners.

4.5 Quality and Management of Web Content

The recommended best practice to ensure quality of content provided on the MDAs/LGs websites are as follows:

1. MDAs/LGs shall ensure that the content created for the website is of high quality, accurate, current and meets the needs of the users and the requirements of the government.

2. MDAs/LGs shall continuously endeavor to create web content that reflect relevancy and currency. Presentation of content shall seek to limit each page to one concept as well as provide information suitable for the web.

3. MDAs/LGs shall ensure that delivering information and services on the Internet is managed with the same level of quality and commitment as that employed when delivering information and services using conventional methods.

MDAs/LGs shall ensure that web content have the following characteristics:

1. Adaptability: Create content that can be presented in different ways without losing information or structure
2. Presentability: Consider the characteristics of created documents and how to best present them. Downloadable versions are recommended for lengthy documents. For PDF files, provide a link to the latest Document Reader.
3. Functionality: Web components shall work correctly and quickly
4. Authenticity: Each document included shall contain the following, but not limited to:
   (a) Status of the document, where applicable
   (b) Author and date
   (c) Version and location of the original publication

(d) Contact details and feedback mechanisms

5. Usability: Website shall be simple and well organized
6. Relevancy: Web content shall be meaningful to the target audiences
7. Distinguishability: Make content easier for users to see and hear including separating foreground from background
8. Operability: All functionality of the content should be operable through a key board interface without requiring further user intervention
9. Readability: Make content readable and understandable
10. Well-written: good grammar and spelling
11. Appearance: shall be appealing to the target audiences
12. Timely: Up to date content
13. Compatibility: Content shall be accessible through the various media, end user devices and across different browser platforms
14. Robustness: Content must be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies.

4.6 Online Viewers/Consumer feedback

MDAs/LGs shall use consumer feedback as a primary indicator of the success of the website. Consumer feedback can help in determining website relevance, usefulness, currency of information and quality. All problems and consumer queries shall be attended to in a timely and professional manner. IT Officers shall be assigned to:

1. Review reported compliments, comments, problems and queries
2. Forward comments, problems and queries to the appropriate office in the MDA/LGs for action
3. Monitor timeliness of corrective action to be undertaken.
4. Respond to the consumer within defined timeframes

4.7 Decommissioning MDA/LG Websites

Government MDAs/LGs shall ensure that websites are regularly reviewed to ensure that they are relevant and up-to-date. An MDA/LGs website shall be retired on the following grounds:

1. When it has been rendered irrelevant due to re-organization of Government MDAs/LGs structures
2. When it does not serve a specific function or purpose of the Government MDA/LGs
3. When it was developed for a particular project or strategy that is no longer relevant or current

4. When it was launched as part of a government-sponsored campaign that has since come to an end

5. Is non-essential and website traffic statistics, where available, shows that the website is not being utilized.

When decommissioning websites, consideration shall be given to archiving the content as appropriate.

4.8 Security and Privacy of MDA/LGs Website

In ensuring MDA/LGs Website security and privacy the following shall be considered:

1. MDAs/LGs shall put in place measures or controls to protect web resources to assure the confidentiality, integrity and availability of information. MDAs/LGs shall ensure that information assets are safely and securely stored, processed, transmitted and destroyed.

2. MDAs/LGs shall develop website security plans and ensure that users are alerted of potential risks and how to avoid them when accessing the website.

3. MDAs/LGs shall ensure that information collected from users through electronic forms or e-mails are securely transmitted and stored by the taking appropriate measure such as data encryption.

4. Reasonable care shall be taken to protect personal information held by MDA/LGs from misuse, loss and unauthorized access, modification or disclosure. Where necessary, user registration for access and use of services such as access to government MDA/LGs databases shall be enforced.

5. MDA/LGs websites shall include a standard privacy policy statement that enumerates information collected about individuals when they visit the website, how it is used. It is important that MDA/LG complies with the undertakings and representations in its website privacy statement.

6. MDAs/LGs shall regularly conduct security threat and risk audits on their websites. They shall also create and regularly review a security plan that describes the necessary security mechanisms and procedures required to secure the website.

4.9 Web Access Platforms

The following shall be considered:

1. MDAs/LGs shall ensure that all websites developed are able to be displayed on all standard browsers. Web services shall be developed for delivery through various access devices mobile telephones, PDAs etc.

2. MDAs/LGs shall ensure that access platforms are adequately secured taking into consideration issues of authentication and repudiation.

4.10 Documentation

MDAs/LGs shall produce and maintain documentation of the development processes, administration and maintenance of the website including internet applications and databases for continuity.

5. INFORMATION TECHNOLOGY EQUIPMENT ROOMS

IT equipment shall be housed in secure IT rooms, protected by well-defined security boundaries, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference which should be in line with the identified risks.

The IT Unit/Department within the respective MDAs/LGs shall be responsible for managing data centers, training rooms, server rooms as well as monitor and review access mechanisms to all IT facilities.

5.1 IT Equipment Rooms and Facilities

The schematic diagram below illustrates the various types of room and the connections between them. This diagram shows an ideal situation for large MDAs/LGs. For smaller institutions one IT room may often contain several functions but it is important to endeavor to create some redundancy for network availability as indicated in the diagram:

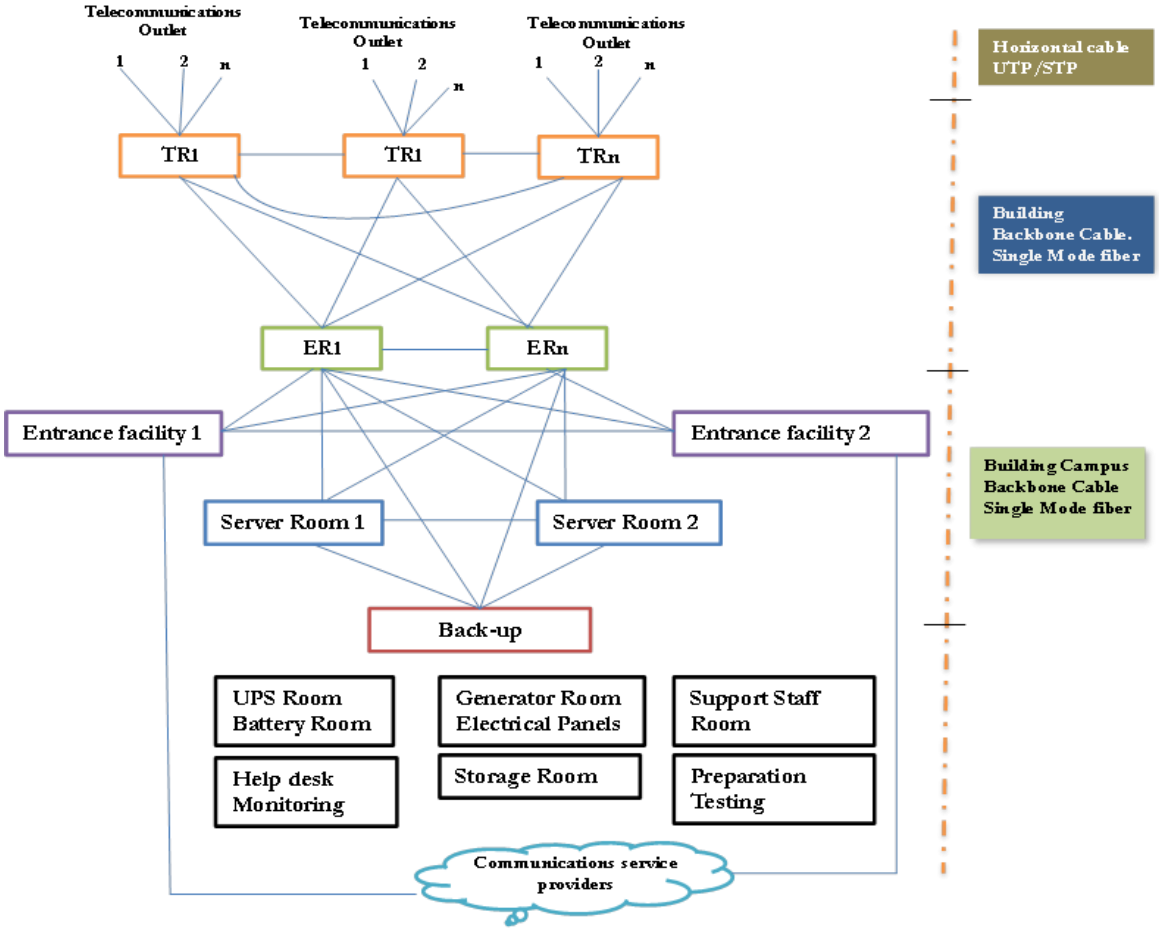


Figure 1 : Schematic Diagram for the different types of Rooms

5.2 Selection and Design of IT equipment rooms

IT facilities supporting critical or sensitive Government services shall be secured in suitable locations and rooms. The following considerations shall be made by MDAs/LGs and Local Governments in the selection of suitable sites for the construction of IT equipment rooms:

1. MDAs/LGs shall take into account reasonable controls and measures to mitigate and guard against natural and man-made disasters including fire, flooding, explosion, vandalism and hazards related to electrical power.

2. Consideration shall be given to the following measures:

   (a) Hazardous materials shall be stored safely at a safe distance from the site. Combustible material such as stationary shall not be stored within the computer room until required.

(b) Fallback equipment and back-up media shall be sited at a safe distance to avoid damage from a disaster at the main site. In particular, Business Continuity Plans and associated equipment shall be stored in a location sufficiently separate to the main location.

(c) Appropriate safety equipment shall be installed in accordance with the Occupational Safety and Health policies/laws in place.

(d) Environmental requirements of an equipment room shall be determined by Manufacturer's specification with due diligence and in consultation with certified professionals.

5.3 Requirement for IT equipment rooms

The requirement shall fall into the following categories:

5.3.1 Security Requirement for IT equipment rooms

The security mechanism to be deployed shall include and not limited to:

1. Access control by use of Bio-metric card logins and passes
2. Alarm systems to counter any unauthorized activity within the vicinity of the IT equipment rooms
3. Security Cameras to monitor activities around the IT equipment room or sites
4. Lockable doors and accessed achieved physical keys.
5. Intrusion detection systems installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows
6. Ensure proper lighting systems are installed to provide clear visibility in and outside the IT equipment room.

5.3.2 Fire Safety Requirement for IT equipment rooms

The following shall be considered in guarding against fires in IT equipment rooms:

1. MDAs/LGs shall consider and ensure that fire and smoke detection systems and systems for detecting environment conditions as well as fire suppression systems are installed in the IT equipment rooms.

2. Fire safety equipment such as gas masks, fire extinguishers and water hydrant facilities shall be installed and located within the vicinity of the equipment room to counteract any fire out breaks.

5.3.3 Power Safety Requirement for IT equipment

The following shall be considered in the provision of power to the equipment.

1. MDAs/LGs shall ensure that the use of smooth energy sources to equipment is adhered too.

2. MDAs/LGs shall use surge protectors to protect equipment against power surges and dips

3. To ensure network availability MDAs/LGs shall ensure that alternative sources of energy exist and that appropriate backup power sources (solar, generators and backup batteries etc.) with appropriate ratings are installed to power up the IT equipment.

4. The supply of fuel to the generator shall be adequate to ensure that the generator can run for a prolonged period.

5. MDAs/LGs shall ensure that the backup power sources are regularly tested, and any necessary requirements included as part of any contingency planning processes.

6. MDAs/LGs shall ensure that proper Uninterrupted Power Supplies (UPS) with appropriate ratings are installed to protect the equipment from power surges

7. Emergency power off switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure.

5.3.4 Cooling Requirement for IT equipment

The following guidelines shall be considered and implemented:

1. MDAs/LGs shall ensure that proper air conditioners/cooling systems with appropriate ratings commensurate with the equipment in place and the size of the equipment room are installed to provide suitable cooling in line with the manufacture requirement or specifications for the equipment.

2. It is important to ensure that the cooling systems are regularly checked for any fault or to fill-up the gas cylinders to provide sufficient cooling.

5.3.5 Construction of IT equipment Rooms

The following consideration shall be made in the construction of IT rooms:

1. MDAs/LGs shall ensure that security barriers such as walls, card controlled entry gates or manned reception desks) are constructed to protect areas that contain information and information processing facilities (IT equipment).

2. The perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur).

3. The external walls of the IT room shall be of solid construction and all external doors shall be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks etc. doors and windows should be locked when unattended.

4. Emergency evacuation procedures shall be developed with due consideration of the security of the IT resources.

5. MDAs/LGs shall make separate considerations for storage rooms for the spare equipment/equipment destined for disposal. MDAs/LGs shall ensure that IT equipment rooms are not used for storage of any kind.

6. Ensure that the IT equipment room is not constructed in or near flood prone areas such as in or near wetlands, swamps and water catchment areas etc.

7. Where the proposed site/location for the IT equipment room is on the first floor or floors above the ground floor the maximum floor load shall be considered commensurate with the total weight of all the IT equipment scheduled to be installed.

8. Ensure that the equipment racks are firmly fixed to the floor of the equipment room to with stand vibration caused by earth quakes or any heavy activity within the vicinity of the equipment room.

5.3.6 IT equipment Safety Requirement

MDAs/LGs shall ensure that all IT equipment is protected from physical and environmental threats. Appropriate measure shall be put in place to protect equipment against physical threats and environmental hazards. The following considerations shall be made in ensuring the safety of IT equipment:

1. IT equipment containing sensitive data should be positioned in restricted areas to reduce the risk of information being accessed and viewed by unauthorized persons during their use and storage.

2. IT equipment demanding special protection should be isolated/secluded and securely protected against any potential unauthorized access.

3. Controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism among others.

5.4 Cabling Infrastructure Security

MDAs/LGs shall ensure that power or cables carrying data or supporting IT technology services shall be adequately protected from interception or damage. The following guidelines shall be considered in the implementation of cabling security:

1. Power cables should be segregated from cables carrying IT services or data to prevent interference

2. Network cables or cables carrying IT Services shall be clearly identified and marked to minimize errors during handling and patching

3. IT units shall ensure that the patch cables used to connect equipment/carrying specific IT service are well documented for ease of reference during maintenance.

4. IT Units shall ensure that cables are installed in armored conduits especially for critical IT services and systems.

5. MDAs/LGs shall ensure that the inspection and termination boxes for all cabling system are securely locked.

6. Ensure controlled access to all installed patch panels, power or data cables rooms.

5.5 Management Information and Audits

1. IT Units within the respective MDAs/LGs shall monitor all aspects of connections over the network. The use of network monitoring tools shall be employed to automate the auditing tasks needed and complement manual auditing. Auditing shall include the following:

    (a) Authentication database showing the specific login entries;

    (b) All entity router/network device configurations;

    (c) Client equipment where tampering may be reasonably suspected;

    (d) Bandwidth management;

    (e) Monitoring of access points;

    (f) Monitoring unauthorized use of network and network facilities.

2. The IT Units shall immediately investigate and document any unauthorized changes whenever detected.

3. All MDAs/LGs connections shall be reviewed on regular basis, by mutual agreement. The IT units shall come up with and document routine maintenance processes. The unit shall come up with SLA for maintenance of network resources with external service provider and ensure that they are adhered to.

5.6 Security Requirement for IT equipment and Information

Detailed requirement for Information and equipment security shall be adhered to as provided in the in the International Standards; *ISO/IEC 27002: Information technology — Security techniques — Code of Practice for information security management. The International standard has been adopted as National IT Standards through Uganda National Bureau of Standards.*

MDAs/LGs shall make reference and adhere to the above international standards which provide best practice guidelines for Information Security management of IT resources.

6. IT EQUIPMENT AND SOFTWARE MANAGEMENT GUIDELINES

6.1 Hardware Management guideline

IT hardware must be treated with care and used with the proper operating instructions. No equipment shall be used which is labeled out of order. Any apparent fault with hardware should be reported promptly to the IT unit within each of the respective MDAs/LGs. IT equipment must not be used if there is reason to believe that it may not be in safe working order.

6.1.1 IT equipment User Responsibility

Users of IT equipment in all MDAs/LGs including local Governments shall observe and adhere to the following guidelines:

1. Users must not access and/or attempt to access any equipment, software and/or data which they are not properly authorized to access. In particular, the confidentiality of data belonging to other users must be respected.

2. Users must not by any deliberate or careless act or omission jeopardize or seek to jeopardize the integrity of any IT equipment, and/or its software and/or any information stored within it and/or accessed through it.

3. Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. Users must not use access codes that belong to someone else.

4. Users must not use any IT equipment for a purpose other than that for which they are authorized. Users must seek advice if they have any doubt about their authority to use any of the IT facilities.

5. Users of IT equipment must take all reasonable steps to exclude and avoid the spread of malicious software such as virus, worms, and must co-operate fully with the IT unit to prevent the spread of such malicious software.

6. End-users of the hardware must not install any software obtained from a third party source or downloaded software, unless such software has been previously checked and cleared of the presence of malicious software by IT unit technical persons. It is an offence knowingly to corrupt a computer program or any of the data stored in the computer system.

7. IT equipment must not be used to download pornographic, obscene, excessively violent and/or offensive materials from the Internet

6.2 Software Management and Usage Guidelines

NITA-U recommended the use of licensed Software from recognized partners in Uganda. The software developer usually copyrights such software and, unless expressly authorized to do so, MDAs/LGs have no right to make copies of the software. The purpose of this guideline is to prevent copyright infringement and to ensure proper software asset management.

6.2.1 MDAs/Local Government Responsibilities

1. It is the responsibility of each MDA to respect and adheres to all computer software copyrights and to adhere to the terms of all Software licenses, manage its software assets and to ensure that it installs and uses only legal software on its desktop computers (including portables) and servers.

2. MDAs/LGs and local Governments shall ensure that necessary steps are put in place to prohibit users from duplicating any licensed software or related software.

3. MDAs/LGs shall ensure that software acquisition, copy, distribution, transmission and use is in accordance with the terms and conditions in stipulated in the license agreement accompanying that particular software product.

6.2.2 IT hardware and Software Acquisition

1. MDAs/LGs shall ensure that only legitimate software must be provided to all system users who need it. All requests for IT hardware and software including upgrades must be submitted to the IT unit. All software and hardware acquired by MDAs/LGs must be approved and purchased through the IT unit. Software must be purchased only from reputable, authorized software vendors and suppliers approved by NITA-U.

2. Where hardware and software is acquired through other means for example given free by implementing partners, the IT unit should be notified for documentation purposes.

3. MDAs/LGs shall ensure that hardware and software acquisition channels are restricted to ensure that it has a complete record of all her hardware and software that has been purchased for and can register, support, and upgrade such products accordingly.

6.2.3 Software Installation Guidelines

After the legal acquisition of the software the following installation guidelines must be observed.

1. Only personnel from the IT unit are recommended to carry out software installation on the MDA/LG computers, laptops and the network.

2. Only those persons explicitly authorized by the MDA/LG to install software may install software on the organization's computers and servers. Such persons shall not do so unless and until he/she has first obtained an appropriate license for that software.

3. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

6.2.4 Storage of Software and Documentation

1. MDAs/LGs through the IT unit shall ensure that the original software media is kept in a safe storage area maintained by the designated department.

2. The designated department shall in addition store all original software licenses and registration and purchasing information in a safe storage area.

3. MDAs/LGs shall ensure that user manuals are provided, must reside with the IT unit but may be loaned to users if the IT unit keeps records of who has borrowed the manual. The IT unit shall destroy all copies of software that are obsolete or that the MDA is no longer licensed to use.
4. The IT unit in each MDA shall keep and maintain a register of all organization's software. The register must contain:
    (a) Title and publisher of the software
    (b) Date and source of Software acquisition
    (c) Location of each installation
    (d) Software product's key number

7. MAINTENANCE AND REPAIR OF IT EQUIPMENT

This section provides best practices and guidelines for scheduling and performing maintenance operations on IT equipment and systems.

It further gives the fundamental steps to build a consistent IT maintenance system, which are as follows:

1. Maintenance planning and contracting (implement hardware/software/data/ inventories, prioritize needs)

2. Schedule/Monitor Maintenance Activities

7.1 Preparation for Maintenance of IT equipment

IT Maintenance is considered as the set of all actions which have as an objective to retain an item (or the whole system) in, or restore to, a state in which it can perform the required function. The actions include the combination of all technical and related administrative, managerial, and supervisory actions such as tests, measurements, replacements, adjustments and repairs.

MDAs/LGs shall adhere to the following general guidelines in preparation of IT equipment for maintenance:

1. An efficient record/inventory keeping of the IT equipment/systems in hand is essential for maintenance management; hence performing a hardware, software and telecommunications inventory is the first step of an efficient maintenance program. Keep an inventory of all IT equipment in the MDA/LG, and give periodic (quarterly, half year or annual) reports of equipment status.

2. Conduct surveys to identify obsolete equipment for the purposes of disposal, replacement or repair. IT personnel shall ensure that data is permanently erased using suitable mechanism from IT equipment destined for disposal.

3. MDAs/LGs shall conduct a data preservation survey to indicate volumes, importance and retention period of data, which in turn results to decisions about data retention periods, backups and requirements on availability and security especially for equipment scheduled for maintenance.

4. MDAs/LGs shall within the IT Unit establish a maintenance function to regularly assess the status of IT equipment and schedule for maintenance accordingly. It is important to ensure that IT equipment maintenance is conducted in-house as this reduces the changes of unauthorized access to data or information or loss and damage of equipment.

5. The IT Units within the MDAs/LGs shall develop a maintenance schedule and upgrade plans of all IT equipment.

6. Sub-contracting for maintenance shall be through appropriate justification and approval by the Accounting Officers. Due diligence shall be undertaken in retaining such contractors.

7. MDAs/LGs shall ensure to train and build the capacity of IT personnel to conduct maintenance activities on IT equipment.

8. MDAs/LGs shall ensure that appropriate maintenance reporting mechanisms are in place. This shall include a standard format for reporting, administrative structures to address maintenance issues as well as sourcing for maintenance of IT equipment.

9. IT equipment scheduled for maintenance shall be tagged with the standard MDA/LG labeling conventions and appropriately physically secured.

IT maintenance may be distinguished as Preventive and Corrective. The following section outlines the best practices to be adopted in each category to address maintenance issues of IT equipment.

7.2 Preventative Maintenance

Preventive maintenance aims at retaining the IT equipment or Software capabilities before the occurrence of any problem such as systems failure or equipment breakdown. Identifying and performing minor and safety repairs in a timely fashion helps to ensures equipment availability and integrity.

Preventive maintenance is the care and servicing by maintenance personnel to keep facilities in a satisfactory operational state by providing for systematic inspection, detection, and correction of incipient failures either before their development into major failures or before their occurrence

Performing preventive maintenance has several objectives which include improving capital equipment's productive life, reducing production losses caused by equipment failure, minimizing critical equipment breakdowns, and improving the health and safety of maintenance personnel.

7.2.1 Elements of Preventive maintenance

The table below describes the fundamental elements of preventive maintenance which should be considered and included in the maintenance plan and implemented by the MDAs/LGs.

Table 1: Elements of Preventive Maintenance

No.	Elements	Description of Element	Responsibility
1	**Inspection**	Periodically inspect items to determine their serviceability by comparing their physical, mechanical, electrical, and other characteristics to established standards.	IT Units / Designated Personnel
2.	**Calibration**	Detect and adjust any discrepancy in the accuracy of the material/component or parameter being compared to the	"

		established standard value.	
3.	**Adjustment**	Periodically make adjustments to specified variable elements of the IT equipment to achieve optimum performance	"
4.	**Testing**	Periodically test to determine serviceability and detect mechanical or electrical degradation	"
5.	**Servicing**	Periodically charge, and clean/dust etc. materials, components or items to prevent the occurrence of incipient failures	"
6.	**Installation**	Periodically replace limited-life items or IT equipment experiencing wear or degradation to maintain the specified tolerance level.	"
7.	**Alignment**	Make changes to an item's/IT equipment specified variable elements to achieve optimum performance	"

Preventive maintenance activities may include but not be limited to the following:

(a) Virus scanning

(b) Active directory scanning

(c) Data volume control and compression (if applicable)

(d) Data archiving/purging

(e) Hard discs bad blocks detection and replacement

(f) Batteries charging or replacement to prevent

(g) Sealing of leakages in equipment rooms

(h) Replacement of leads on broken cables, fuses

(i) Regular physical inspection of IT equipment for any potential source of damage and avoiding the actual occurrences of breakdown.

(j) Inspection of power sources for any potential cause of short circuits/power outages and the immediate replacements and inspection of fuel gauges on generators before the fuel run out among others

MDAs/LGs shall ensure and encourage scheduled preventive maintenance actions that prevent premature failure or extend the useful life of an IT asset, or systems and components and that are cost-effective on a life-cycle basis.

7.2.2 Preventive Maintenance Program

MDAs/LGs shall develop a preventive maintenance program by considering the following:

1. IT Units within the MDAs/LGs shall identify all IT equipment, systems and components to be included in the maintenance Program. The list of identified IT equipment is not intended to be an exhaustive list of every component but comprehensive and all inclusive.

2. The IT Unit within the MDA/LG shall develop a detailed inventory to quantify the IT equipment, systems and components and to establish their current condition through facts gathering or assessment. Information gathered from the condition assessment is used to determine both the immediate and future levels of preventive maintenance for the system or component and its end-of-service-life replacement date.

3. Information such as quantity, type, size, manufacturer, model, material specification, location, key parts, part numbers, and other item-specific data shall be documented by the IT Units.

4. Determine the levels of maintenance required by establishing the basic life-span for the IT equipment and components and the actual maintenance activities required for the equipment to meet or exceed the life expectancies.

5. Analyze manufacturer's literature, test results, industry averages and benchmark experiences from the use of similar IT equipment to determine acceptable life-cycles and preventive maintenance measures needed to achieve those life expectancies in the most efficient manner.

6. Once the levels of maintenance have been established IT Units within the respective MDAs/LGs shall ensure that a work plan for Preventive Maintenance is prepared and adhered to and shall include frequency and nature of work to be conducted and the materials/tools to be used. A preventive maintenance plan shall include:

    (a) Computerized maintenance management program or other formal systematic means of tracking the timing and costs associated with planned and completed maintenance activities, including scheduled preventive maintenance.

    (b) Addresses energy management for all IT equipment in use within the MDA/LG

    (c) A regular custodial care program for the IT equipment within the MDA/LG

    (d) Preventive maintenance training for IT maintenance personnel and staff within the MDA/LG

(e) Renewal and replacement schedules for electrical, mechanical, structural, and other components of facilities owned or operated by the MDA/LG.

The table 2 below provides a summary of the fundamental steps for developing a highly effective Preventive maintenance Program.

Table 2: Steps to develop effective Preventive Maintenance Program

No.	ACTIVITY	ACTIVITY DESCRIPTION
1.	**Identify and select the areas**	Identify and select of one or two important areas on which to concentrate the initial preventive maintenance effort. The main objective of this step is to obtain good results in areas that are highly visible
2.	**Highlight the preventive maintenance requirements**	Define the preventive maintenance needs and then develop a schedule for two types of tasks: (1) Daily preventive maintenance inspections (2) Periodic preventive maintenance assignments.
3.	**Determine assignment frequency**	Establish the frequency of assignments and review the item or equipment records and conditions. The frequency depends on factors such as: (1) Vendor recommendations (2) Experience of personnel familiar with the equipment or item under consideration, (3) Recommendations from engineers.
4.	**Prepare the preventive maintenance assignments**	Prepare the daily and periodic assignments in an effective manner and then get them approved.
5.	**Schedule the preventive maintenance assignments**	Schedule the defined preventive maintenance assignments on the basis of quarterly, half year or annual period
6.	**Expand the preventive maintenance program as appropriate**	Expand the preventive maintenance program to other areas on the basis of experience gained from the pilot preventive maintenance projects.

7.2.3 Implementation of Preventive Maintenance Program

In implementing the Preventive Maintenance Program, the following guidelines shall be adopted:

1. MDAs/LGs through the IT Units shall determine and dedicate resources (financial and skilled human resource) required for successful implementation of the maintenance activities/program.

2. MDAs/LGs shall establish the required structure and organization of the maintenance activities before scheduling and apportioning any related works. These may include identification of skilled personnel to conduct maintenance, location where the to conduct such activities etc.

3. Upon establishing the required maintenance structures/team, the IT Units in the respective MDAs/LGs shall schedule and assign maintenance work accordingly using a work order system or job cards.

4. MDAs/LGs shall establish a reporting and feedback system/procedures to help IT personnel report and track the status of IT equipment as well as the maintenance activities. This process may be automated by implementing a maintenance management software program to generate reports etc.

7.3 Corrective Maintenance

Corrective maintenance is the remedial action performed because of failure or deficiencies found during preventive maintenance or otherwise, to repair an item to its operating state. Normally, corrective maintenance is an unplanned maintenance action that requires urgent attention that must be added, integrated with, or substituted for previously scheduled work. Corrective maintenance or repair is an important element of overall maintenance activity.

Corrective Maintenance may fall under the following categories which must be considered by the MDA/LG specifically by the IT Unit/personnel conducting the Corrective maintenance activities.

7.3.1 Categories of Corrective Maintenance

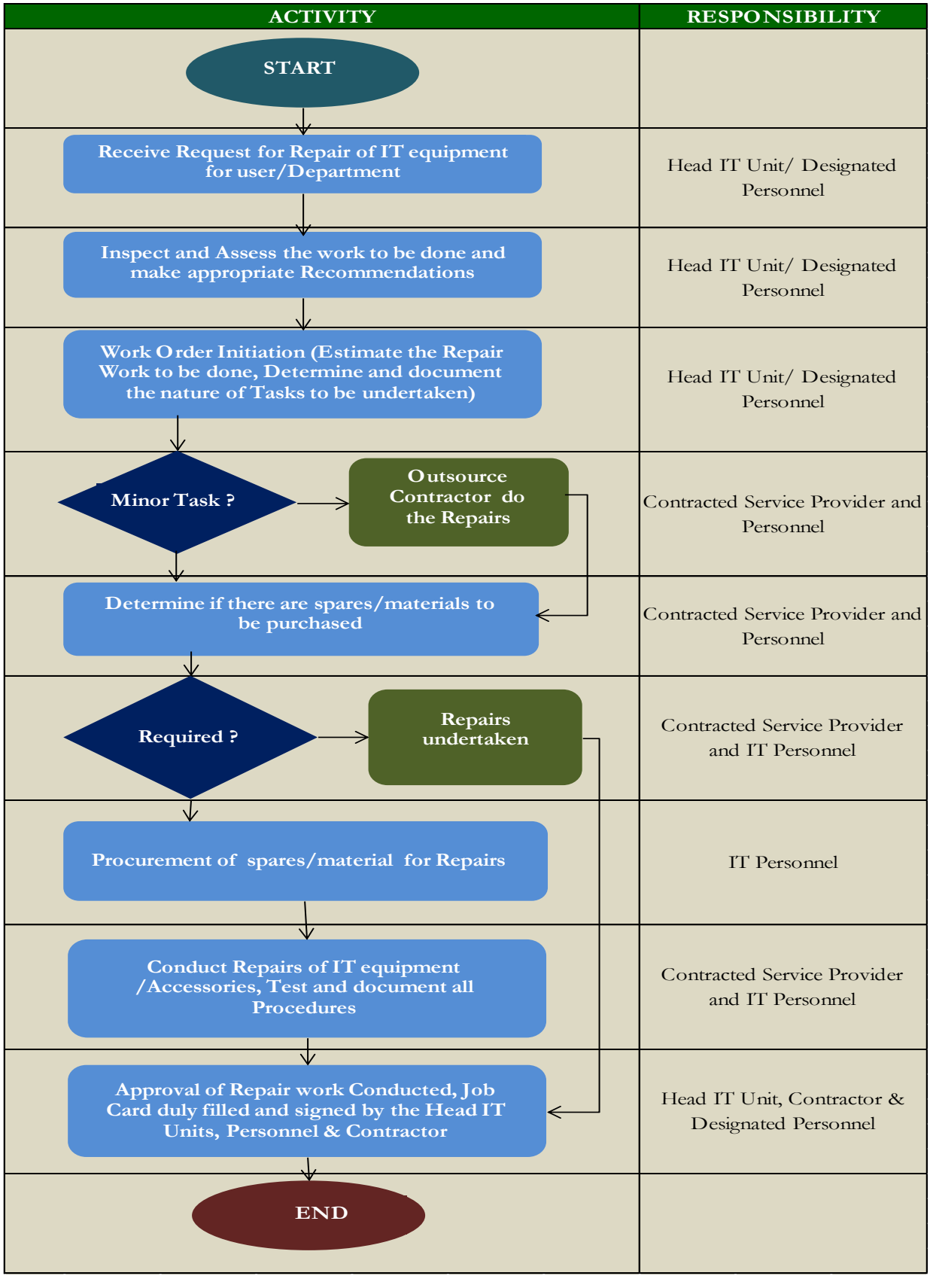
Corrective maintenance may be categorized as highlighted in the table 3 below:

Table 3: Categories of Corrective maintenance

No.	Category	Description of Categories of Corrective Maintenance	Maintenance Actions
1.	**Fail repair**	This is concerned with restoring the failed item or equipment to its operational state.	• Replace/upgrade failed parts according to manufacturer specification
2.	**Overhaul**	This is concerned with repairing or restoring an item or equipment to its complete serviceable state meeting requirements outlined in maintenance serviceability standards, using the "inspect and repair only as appropriate" method.	• Upgrade/replace/refurbish all parts of the IT equipment upon inspection
3.	**Salvage**	This is concerned with the disposal of non-repairable materials and utilization of salvaged materials from items that cannot be repaired in the overhaul, repairs, or rebuild programs.	• Dismantle non-repairable items/equipment and re-use components in other repairable IT equipment
4.	**Servicing**	This type of corrective maintenance may be required because of a corrective maintenance action; for example, generator engine repair can result in requirement for crankcase refill, welding etc.	• Lubricate moving parts, tighten the bolts and screws, replace worn out parts and damaged cables etc.
5.	**Rebuild**	This is concerned with restoring an item or equipment to a standard as close as possible to its original state with respect to appearance, performance, and life expectancy	• Completely disassemble /dismantle IT equipment • Examine of all parts of equipment • Replace/repair unserviceable parts and worn out components according manufacturer specification/tolerance • Test to the original production requirement

7.3.2 Steps for Conducting Corrective Maintenance

The recommended steps for conducting corrective maintenance of IT equipment and related accessories are as indicated by the flow chart in the figure 2 below:


ACTIVITY
RESPONSIBILITY
START
Receive Request for Repair of IT equipment for user/Department
Head IT Unit/ Designated Personnel
Inspect and Assess the work to be done and make appropriate Recommendations
Head IT Unit/ Designated Personnel
Work Order Initiation (Estimate the Repair Work to be done, Determine and document the nature of Tasks to be undertaken)
Head IT Unit/ Designated Personnel
Minor Task ?
Outsource Contractor do the Repairs
Contracted Service Provider and Personnel
Determine if there are spares/materials to be purchased
Contracted Service Provider and Personnel
Required ?
Repairs undertaken
Contracted Service Provider and IT Personnel
Procurement of spares/material for Repairs
IT Personnel
Conduct Repairs of IT equipment /Accessories, Test and document all Procedures
Contracted Service Provider and IT Personnel
Approval of Repair work Conducted, Job Card duly filled and signed by the Head IT Units, Personnel & Contractor
Head IT Unit, Contractor & Designated Personnel
END

7.3.3 Strategies for effective Corrective Maintenance

To improve corrective maintenance effectiveness, it is important to reduce corrective maintenance time. Below are some of the useful strategies for reducing system-level corrective maintenance time.

1. MDAs/LGs shall ensure that limited time is spent accessing spare parts of IT equipment. It is important to purchase equipment with their spares or have knowledge of where to purchase spares within a limited time frame to prevent prolonged down times.

2. Effective functional and physical interchangeability is an important factor in removing and replacing parts or components, thus lowering corrective maintenance time.

3. Improve fault recognition, location, and isolation by adopting good maintenance procedures, utilizing well-trained maintenance personnel, well-designed fault indicators, and unambiguous fault isolation capability this will reduce the corrective maintenance times.

4. Create awareness among staff for proper selection, use of indicators and dials, about the size, shape and weight of components, readability of instructions, use of information processing aids etc. this will help reduce corrective maintenance time.

5. MDAs/LGs shall ensure to employ/redundancies especially for mission critical IT systems and infrastructure; this will reduce corrective maintenance time.

7.4 Software Upgrade Guidelines

It is important to keep in mind that upgrading either the system or the application software may result to some inconsistencies within the total system. Not all applications can run effectively under any versions/releases. Furthermore, application upgrades may also require database upgrades etc.

It is always recommended to:

1. Maintain a development environment, where new software releases can be tested for possible inconsistencies or malfunctions, before they are applied to the production environment.

2. Back-up all data before proceeding to software upgrades

7.5 Maintenance of IT Equipment

All MDAs/LGs and Local Governments shall ensure that IT equipment installed in their respective institutions is correctly maintained to ensure continued availability and integrity.

During maintenance of IT equipment MDAs/LGs shall ensure that:

(a) IT equipment are maintained in accordance with the supplier's recommended service intervals and specifications;

(b) Only authorized maintenance personnel carry out repairs and service equipment and that records of all maintenance activities should be kept for all suspected or actual faults, and all preventive and corrective maintenance conducted;

(c) Appropriate measures and controls are implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the Institution; where necessary, sensitive information should be cleared from the equipment, or the maintenance personnel should be sufficiently cleared to carry out the maintenance activities

(d) MDAs/LGs shall ensure that equipment for maintenance should not be taken off-site without prior authorization;

(e) MDAs/LGs shall ensure that staff, contractors is fully identified during equipment removal for maintenance of assets should be clearly identified;

(f) MDAs/LGs shall set time limits for equipment removal for maintenance and returns checked for compliance;

(g) Where necessary and appropriate, equipment should be recorded as being removed from the site and recorded when returned.

7.5 General Guidelines for Maintenance of IT equipment

The following are some of the general guidelines for the use in the maintenance of IT equipment across MDAs/LGs:

1. IT Unit within each MDAs/LGs shall develop a yearly plan for preventive maintenance, indicating the responsible person for each activity and monitor the activities as appropriate.

2. For safety reasons, it is important that backup data is kept in a safe place outside the building where the installation resides.

3. MDAs/LGs through their IT Units shall ensure that accurate and comprehensive documentation (including design documents) are put in place to enhance maintenance programs. Details to the adjustments and upgrades made on the IT equipment and software must be properly recorded and maintained including inventory of all equipment in the MDAs/LGs.

4. MDAs/LGs through their IT Units shall maintain a development environment where new versions/releases of both system and application software before deployment can be tested.

5. MDAs/LGs shall ensure that equipment maintenance and upgrades are channeled through the IT Units to evaluate the request, resolve it if possible or escalate it to the maintenance contractor.

6. Monitoring maintenance activities is a major task of System Administration activities, and provides significant data about overall system quality and costs.

7. Preventive maintenance should be encouraged to keep equipment and facilities in satisfactory operating condition by providing for systematic inspection, detection, and correction of incipient failures either before they occur or before they develop into major defects.

8. MDAs/LGs shall ensure that the IT Units are trained with the right skills to maintain equipment and properly handle the upgrade of software and systems.

8. HUMAN CAPACITY DEVELOPMENT

8.1 End User Skills Development

It is important to note that the dynamic nature of IT requires necessary skills to ensure optimum utilization of the services/systems, keep them running and implementing them demand new and high-level skills.

In the development of human capacity to use the IT infrastructure adequately in service delivery, all MDAs/LGs shall consider the following:

1. It is the responsibility of the MDAs/LGs and Local Government to promote the deployment of IT in all programs at all levels in the broadest sense. MDAs/LGs needs to ensure and requires that all staff are trained on a continuing basis to equip them with adequate skills to fully exploit the IT environment in their different functions.

2. MDAs/LGs shall ensure that end-user skills development includes all efforts to enforce awareness, general knowledge and specific computer skills related to the use of information technology. Within this context, the end user is defined as each person who uses IT services to enhance on his/her daily office work. Staff training on the usage of IT should therefore be given high priority.

3. MDAs/LGs shall ensure that staff is trained and equipped with skills to:

(a) Use IT services and systems effectively and as independently as possible
(b) Establish and sustain effective, efficient application and data management and system maintenance
(c) Be aware of the shared responsibilities for equipment, software and data and enforce an atmosphere of collective responsibility and system ownership.
(d) Contribute to the specification, design and implementation of IT applications

4. MDAs/LGs shall ensure that policies are in place that provides for the development and implementation of a consistent set of training programs with different categories of IT users. These include among others management staff, head of departments, program officers, administrative assistants and contract volunteers. Training should be provided to cover, as far as possible all skill levels.

5. While it is not intended to turn all users into experts, it is important that the training plan supports all users of IT at all levels. The short- and medium term goals shall aim at creating, as rapidly as possible, a sizeable proportion of staff that are familiar with and are able to effectively use the IT infrastructure in their daily work. At the end of the training, MDAs/LGs expects that:

   (a) All staff at all levels are able to use standard application packages (Word, Excel, Power Point, Publisher, and Access) as well as Email and Internet with ease.

   (b) Administrative chores such as calling meetings and distribution of minutes and other documents are handled via e-mail.

   (c) All official correspondents via e-mail be handled using the MDAs/LGs email accounts for respective programs.

REFERENCES

1. Requirements for the Design of ICT rooms (Best Practice Documents)
   http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs103.pdf

2. Fire Prevention Requirements for ICT rooms (Best Practice Documents)
   http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs104.pdf

3. Information and Communication Technology (ICT) Standards and Guidelines
   http://www.access-board.gov/attachments/article/490/draft-rule.pdf

4. ISO/IEC/27002: Information technology — Security techniques — Code of practice for information security management

5. ICT Standards and Guidelines(Directorate of e-Government-Kenya)
   http://www.e-government.go.ke/

6. Maintainability, Maintenance and Reliability for Engineers
   http://www.media.rmutt.ac.th/media/eBook/Engineer/Maintenance/Maintainability,%Maintenance,%20and%20Reliability%20for%20Engineers/7243_C000.pdf