JAMHURI YA MUUNGANO WA TANZANIA

OFISI YA RAIS,
MENEJIMENTI YA UTUMISHI WA UMMA

Mwongozo wa Matumizi Bora, Sahihi, na Salama ya Vifaa Na Mifumo ya Teknolojia ya Habari na Mawasiliano Serikalini

Toleo la Pili, 2015

Umetolewa na Ofisi ya Rais, Menejimenti ya Utumishi wa Umma

Oktoba, 2015

TABLE OF CONTENTS

ABBREVIATIONS

Abbreviation	Explanation
CD	**Compact Dic**
DVD	Digital Versatile Disc
ICT	Information and Communication Technology
eServices	Electronic Services
G2C	Government to Citizens
G2B	Government to Businesses
G2E	Government to Employees
G2G	Government to Government
e-GIF	e-Government Interoperability Framework
e-Payment	Electronic Payment
ESB	Enterprise Service Bus - A flexible connectivity infrastructure platform for integrating applications and services.
ROM	Read Only Memory
SOA	Service Oriented Architecture - An architectural pattern in information systems design in which application components provide services to other services via a communications protocol, typically over a network.
GPT	Government Project Team

ACRONIMY (DEFITION OF TERMS)

FOREWORD

The rapid growth of Information and Communication Technology (ICT) has changed to a large extent operations of the government and society at large. This growth has facilitated improved Government processes and improved service delivery to citizens. Despite the mentioned advantages there have been challenges in the Government especially in the effective use of ICT. To address the challenges the Government through circular No. 5 of 2009 and it's respective Guideline "*Matumizi Bora, Sahihi na Salama ya Vifaa na Mifumo ya Teknolojia ya Habari na Mawasiliano*" issued directives and guidance on effective and safe use of ICT equipment and systems in the Government.

Despite these efforts, the field of ICT is continually evolving and changing with the advent of new and more advanced ICTs thus needing a more sophisticated approach to address these changes while enhancing coordinated adoption of ICT in the government.

This second version of the guideline is therefore intended to provide a more coordinated and citizen-driven focus for the adoption of the evolving ICT initiatives amongst Public Institutions. Therefore this guideline directs how to implement critical and high level e-Government focus areas identified by the Government to enhance effective usage and adoption of ICT in the Government.

The government has categorized e-Government standards and guidelines in nine areas. These areas are e-Government architecture vision, Interoperability, Business, Application, Information, Integration, Infrastructure, ICT security, ICT processes and Governance. This guideline therefore provides emphasis to employers and public servants to follow standards and guidelines in their daily use of ICT.

It is the hope of the Government that this guide will be used to the fullest by all Public Institutions to bring about positive achievements and at the same time ensuring that Government information is secured despite of ICT usage. Finally, correct application of technology will help Government reduce operating costs and increase efficiency as well as facilitate access to services for citizens and other stakeholders.

HAB Mkwizu

PERMANENT SECRETARY (ESTABLISHMENTS)

Introduction

The Government of Tanzania, through the President's Office – Public Service Management (PO-PSM) established the National e-Government Strategy to enable a more coordinated and citizen-driven focus on e-Government initiatives. The Government aims to leverage on full potential of ICT to achieve good governance, and social and economic development by establishing effective, systematic, and productive e-Government and also improve the efficiency and capability of government processes and services.

The Government has developed e-Government Standards and Guidelines that will address a consistent set of principles which will guide public institutions in the design, acquisition, implementation and management of e-Government projects. In addition, the standards and guidelines will enable interoperability of the systems for better coordination among public institutions, design better projects to avoid redundancy and save costs while investing in new systems and sharing of information for public administration processes.

This document provides Government's directives and easy translation on how to implement the e-Government Standards and Guidelines. It has 9 sections, each with specific theme of e-Government related standards and guidelines. The **first section** is about the e-government standards and guidelines vision in which important directives related to the whole of government, government services, data, applications and technology reference models are defined.

The **second section** issues directives regarding interoperability for government to share, collaborate, integrate information and organised its processes by use of common open standards.

The **third section** provides directives related to the delivery of services by government that are critical, flexible and sensitive to citizen needs as well as those common services which can be re-used by other public institutions.
Well
The **fourth section** provides directives on application architecture in Government. This includes areas of application usability and simplicity, service orientation, adherence to open standards, reusability, flexibility, extensibility.

The **fifth section** elaborates on the information architecture directives for data creation, availability, ownership, security and confidentiality, archival and retention, use of common data and metadata definition and standards.
The **sixth section** provides directives on the integration architecture such that various applications within public institutions are integrated to enable real-time seamless information exchange across government.

The **seventh section** relates to security architecture and provides directives on how to securely and economically protect the public institutions from security threats while maintaining compliance with the security and legal requirements for confidentiality, privacy, accessibility, availability, and integrity.

The **eighth section** provides directives on technology infrastructure supporting government operations such as server, workstation, storage and network infrastructure, software licensing, ICT disaster recovery and business continuity, ICT vendor management, manpower and service management aspects.

The **last section** of this guide defines the set of recommended governance mechanisms through which e-government related standards and guidelines are driven from national level and adopted and implemented at a public institution level.

All public service institutions are directed to make use of this document and other related standards and guidelines to increase their effectiveness and efficiencies in the design, acquisition, implementation and management of e-Government related initiatives. The e-Government related standards and guidelines will be regularly updated and published based on technology change, needs and requirement of the Government by respective Institution.

1. e-Government Standard and Guideline Vision

1.1. Current Situation

As part of the Tanzania e-Government Strategy, 2013, the Government of Tanzania has established an e-Government Strategic Vision: "To be an effective and better government, providing innovative public service delivery enabled by ICT". To realise this vision, Public Institutions need to
Interconnect, support data exchange, share and re-use data within their ICT systems and ensure safe access and exchange of information. The absence of clear e-Government standards vision has led to haphazard development and deployment of e-government systems by Public Institutions without adequate attention to the need to connect, exchange, share and re-use data with other ICT systems therefore hampering the delivery of effective public e-Services. Public Institutions have to elaborate their respective e-Government standards vision to provide a more coordinated and citizen-driven focus for the Tanzania e-Government initiatives.

1.2. Institutional General ICT Rules Development

1.2.1. Public institutions shall develop Institutional general ICT rules. These are high level directives giving instructions on how ICT in the respective Institution can be managed.

1.2.2. Public Institutions shall make reference to the standards on the creation of *General ICT Rules* as described in the *e-Government Vision Standards* and consult with eGA for further guidance.

1.3. Institutional ICT strategy Development

1.3.1. Public Institutions shall prepare ICT strategic plan and ensure that each system or ICT project that is expected to be placed in an institution is in the ICT strategy and / is part of the e-Government strategy. This measure will avoid the purchase of ICT equipment and/ systems due to vendor/ supplier/ donors influence and thus reduce costs that the Government incurs for maintenance and support of these systems and / equipment.

1.3.2. To enhance this public Institutions shall refer to the *ICT strategy* as described in the *e-Government Architecture Vision - Standards* and consult with eGA for further guidance.

1.4. Institutional Enterprise Architecture Development

1.4.1. Public Institutions shall develop their Institutional Enterprise Architecture, this will enhance integration of their business strategy plans and ICT strategy and hence enable using ICT strategically for optimal business realization using ICT and improving public service delivery.

1.4.2. To enhance the development of the Institutional Enterprise Architecture, public Institutions shall refer to Institutional EA standards as described in the e-Government Architecture Vision - Standards Ref No: eGA/EXT/ARC/001 and consult with eGA for further guidance.

2. e- Government Interoperability Framework (e-GIF) Guidelines

2.1. Current Situation

e-Government Interoperability provides a set of instructions for the government to share, collaborate and integrate information by use of common standards for process, data and technology. The challenge of e-Government lies in the exchange of information and coordination within government.

2.2. General Interoperability Considerations

2.2.1. Public Institutions shall comply with interoperability procedures as defined in e-Government Interoperability Standards document to enable the following:

i. interconnection and communication with other government agencies over networking environment,
ii. public service users to effectively access, collaborate, share information and services electronically,
iii. interaction and integration with other Public Institutions both internally and externally for information sharing and exchange, and
iv. secure exchange of information and delivery of services.

2.2.2. The use of open standards shall be given preference over proprietary standards wherever appropriate. In the event of choosing proprietary standards the e-GIF principles shall be considered as the basic requirement.

2.2.3. The institution-based approach shall be replaced by a service-based approach which is closely aligned with e- Government strategy.

2.2.4. In case of private public partnership, the standards for information exchange between the private partner and the Public Institutions shall comply with the e-GIF but flexibility may be allowed in the information

exchange between the partner and the distribution network of the partner reaching the citizens/consumers.

2.2.5. All Public Institutions shall review their technology implementations with the e-GIF, whenever:

i. a new/enhanced /revised version of the e-GIF is released, and/or,

ii. there are new implementations, upgrade of older systems and reviewing their e-Government/e- Services strategy.

2.2.6. All Public Institutions shall mandate compliance to e-GIF in their bidding/Request for Proposal process for any technology product/service intended to be put for use to serve citizens.

2.2.7. Public institutions ICT acquisition process shall be established in such a way that no ICT investment should be made without an approved architecture and compliance to e-GIF.

2.3. Application and Technology Interoperability Considerations

2.3.1. While developing applications, special accessibility needs have to be considered including the provision of more sophisticated and user-specific resources. For instance exceptions should be granted for some applications where alternative approach to achieving interoperability has been agreed amongst all the parties exchanging data.

2.3.2. All future applications and migration of legacy application shall be web based (browser based interface) or any other widely accepted application.

2.3.3. Government mailing system (GMS) or any other Government approved email system shall be recognized as the official means of communication.

2.4. Data and Meta Data Interoperability Considerations

2.4.1. Common language for system communications is mandatory. Public Institutions shall use Extensive Mark-up Language (XML) as the primary standard for data integration and data management for all application.

2.4.2. Data standards, data exchange standards, integration standards are interrelated, Public Institutions shall ensure their compatibility and technical requirements are considered.

2.4.3. Public institutions shall define Data Standard Catalogue which sets out the rationale, approach and rules for setting and agreeing at the set of Government Data Standards (GDS) to be used in the Government Data Schemas and other electronic interchanges of data involving the Public Institutions, developed to support the e-GIF. These standards shall be defined at a logical (business) level and not at a physical database storage

level. It is recommended that they be used for specifying data storage at the Public Institution level. Appendix – Illustration No.2 Template for Data Catalog demonstrates a typical structure/template to define data standards.

2.4.4. Public institutions shall comply with these interoperability standards on Meta data.

2.5. Interoperability Security Considerations:

2.5.1. For Public Institutions interoperability security the following shall be considered:

i. Confidentiality/privacy of government held information
ii. Integrity to continue to exercise control of government data and computing environments
iii. Protect confidentiality rights accorded to personnel who use government systems
iv. Ensure privacy of personal information.

2.5.2. To ensure reliable exchange of information to take place Public Institutions shall comply with e-GIF security related technical standards as referred in the e-GIF standards.

2.6. Interoperability Technical Standards considerations:

2.6.1. Public institutions shall adhere to the following e-GIF Technical Standards as referred in the *e-GIF standards document*

3. Business Architecture Guidelines

3.1. Current Situation

Each public institution currently has its own service delivery model which is either manual, electronic or both methods. However these services exist in silos due to lack of national integrated service delivery platform.

3.2. Business Architecture Considerations

3.2.1. Public institutions shall develop Project management procedures as described in the Business Architecture Standards and Technical Guidelines.

3.2.2. Public Institutions shall interface with Government portal for communicating, presenting and delivery of government services to citizens.

3.2.3. Public Institution must identify, prioritise and deliver services that are critical and flexible to citizens, businesses employees and other Public

Institutions (G2C, G2B, G2E and G2G) needs and consider the ICT in delivering these services.

3.2.4. Public Institutions shall identify common services that could be re-used by the other Public Institutions to avoid duplication.

3.2.5. Government shall implement Public Key Infrastructure (PKI) to ensure legality and authenticity of online transactions.

3.2.6. The Government e-Service Delivery Gateway and Government Portal shall serve as the Service Access Provider that will provide the infrastructure to facilitate access of Government services by the Service Seekers

3.2.7. Public Institutions shall leverage the Government e-Payment mechanisms for electronic transfer of service charges and for receiving fund from the Government into their accounts.

3.2.8. All Public Institutions shall identify their ICT projects and portfolio driven uniquely by their business services and requirements by referring business reference model standard.

3.2.9. Public Institutions shall use social media to reach out to the public with press releases and announcements and to broadcast new services, schemes and programs, educate the public on various good practices (e.g. good healthcare practices, education around AIDS prevention) and seek the public's views and collect feedback.

3.2.10. Public Institutions shall consider using mobile or kiosk based service delivery interfaces at different hot-spots or postal centres to promote service accessibility to the community.

3.2.11. Public Institutions shall adopt a Service Oriented Architecture (SOA) in service delivery.

3.2.12. Public Institutions shall refer to the Business Architecture - Standards and technical guidelines Ref No: eGA/EXT/ARC/003 and consult with eGA for further guidance.

4. Application Architecture

4.1. Current Situation

Application architecture provides the blueprint for the information system deployment, interaction and their relationship to the business processes. This will ensure simplification, reuse and scalable application across Public Institutions. The current application ecosystem of government ranges from custom built through to commercially off the shelf systems. Public Institutions are effectively making the use of these applications for enhancing their internal business operations. However, limited considerations have been given to interoperability, integration, eservices, de-duplication amongst others.

4.2. Application Architecture Considerations

4.2.1. Public Institutions shall design applications with the objective to promote reusability, scalability, simplicity and ease of use.

4.2.2. Public Institutions should adopt open and web based standards for all new systems. Open standards should promote platform independence, vendor neutrality, enable sustainable information exchange, interoperability, flexibility and greater freedom from technology and vendor lock-in.

4.2.3. Public Institutions shall maintain an application portfolio for the core operations and supporting functions. This includes internet and intranet business applications, collaboration and support applications, reporting and business intelligence applications amongst others.

4.2.4. Public Institutions shall refer to the Application Architecture - Standards and technical guidelines Ref No: eGA/EXT/ARC/004 and consult with eGA for further guidance.

5. Information Architecture

5.1. Current Situation

Information architecture focuses on organizing, structuring, and labeling contents of information in an effective and sustainable way with the goal of ease of finding information at a given location. Government data currently resides at Public Institutions level where information is being stored under specific databases. There are no formal data classification and management strategies which lead to ambiguities and inconsistencies in the use of data by each public institution.

5.2. Information Architecture Considerations

5.2.1. Public Institutions shall establish effective data management to ensure effective decision making and improved performance.

5.2.2. Public Institutions shall have a common definition of data to be exchanged across the Government, agreed format and meaning of the data items. A common vocabulary should facilitate effective communications and enable sharing of data.

5.2.3. Public Institutions should adhere to the Government Dictionary of ICT Terms and Definitions on ICT that is freely shared and collectively owned by all Public Institutions.

5.2.4. Public Institutions shall key in information once and re-use it across the Government. This should reduce costs, promote the efficiency, accuracy, consistency of data and assures quality. Readily available data should facilitate timely data access at every level of the Public Institution and provide timely response to information request and effective service delivery.

5.2.5. All Public Institutions shall have an authoritative, official, primary data source that is the location for all create, update and delete actions.

5.2.6. Public Institutions shall identify data owners and point of contact that should be responsible and accountable for all changes in the data entities and data services and the approval of the same.

5.2.7. Public Institutions shall ensure compliance with legislation regarding government data and security rules.

5.2.8. Public Institutions shall classify their data to:

i. Facilitate the exchange of information electronically, and

ii. Establish information exchange formats that can be shared across Public Institutions.

5.2.9. Each Public Institution shall create their own information catalogue with descriptions of strategic business data and information exchanges.

5.2.10. Public Institutions shall refer to the *Information Architecture - Standards and technical guidelines Ref No: eGA/EXT/ARC/005*

6. Integration Architecture

6.1. Current Situation

Integration Architecture provides the guidance on how Public Institutions will integrate their applications such that real time seamless information exchange is enabled across the Government of Tanzania. Currently very limited data exchange across applications is possible in batch mode, extracting data in flat files (excel or word) and uploading in respective business related applications. Most of the Public Institutions applications lack the flexibility to integrate with external third parties systems related to other Public Institutions in real-time mode, leveraging web service based interfacing strategies.

6.2. Integration Architecture Considerations

6.2.1. Public Institutions shall aim to effectively interconnect, collaborate, access and facilitate data integration and communication between G2G, G2C, G2B and G2E.

6.2.2. Integration of services requires means for connecting the services to be defined. Public Institutions shall define the means for connecting the services by using recommended approach such as the *service oriented architecture (SOA).*

6.2.3. Public Institutions shall make use of a set of rules and principles for integrating services such as the *Enterprise Service Bus (ESB)* for providing interaction between service consumers (citizens, employees and businesses) and service providers (Public Institutions).

6.2.4. Public Institutions shall adhere to the guidelines for Web Service Design, Web Service Development and Web Service Performance for any external integration with other Public Institutions as described in the *Integration Architecture - Standards*.

6.2.5. Public Institutions shall consider the integration architecture technical guidelines for Application Integration as described in the *Integration Architecture - Standards*.

6.2.6. Public Institutions shall consider the integration architecture technical guidelines for Data Integration

6.2.7. Public Institutions will identify and agree on common data and metadata standards/format to access, share and integrate data. Standardization will include common vocabulary, metadata and templates for use across Public Institutions.

6.2.8. The Government of Tanzania shall define a government wide XML schema data sharing across the interoperability framework which will be based on the above common data specification.

6.2.9. All Public Institutions that expose their government services such as e-Services shall adhere to the recommended common data exchange specification as defined in the Government Data XML Schema and the exchange package (or web service contract definition) to enable seamless information flow.

6.2.10. Public Institutions shall establish data sharing agreements. An evaluation has to be performed on the required changes in rules at all appropriate levels of government that will be needed to support data sharing agreements.

6.2.11. Public Institutions shall consider the guidelines for Web Service Design

6.2.12. Public Institutions shall consider guidelines for Web Service Development

7. Infrastructure Architecture

7.1. Current Situation

Infrastructure Architecture provides guidance on how Public Institutions should design their Infrastructure to enable a structured, standardized approach which supports integration, interoperability, business process and applications. Most of the Public Institutions do not maintain a formal hardware, workstation and software asset inventory. There is no adequate information available on current network architecture diagrams with respect to the capacity, performance and availability of the existing networks to assess their ability to fulfill the ICT strategy and application services objectives. In general, the ICT service delivery process within Public Institutions is not well documented and structured.

7.2. Infrastructure Architecture Considerations

7.2.1. Public Institutions shall perform adequate sizing of their infrastructure to meet the changing and growing needs of the organisation. Applications and technologies should essentially scale up, to adapt and respond to such requirement changes and demand fluctuations. Server, storage and network capacities must be able to handle user, application and data loads.

7.2.2. Public Institutions shall ensure that the technology infrastructure should exhibit no single point of failure. The system infrastructure should be architected considering failover requirements and ensure a single server or network link failure does not bring down the entire system (although e.g. performance may degrade).

7.2.3. Public Institutions shall monitor the systems health at regular intervals. Public Institutions shall make use of central monitoring system to gauge the health of their applications at all times and monitor against the pre-defined service level agreements.

7.2.4. Public Institutions shall adhere to Infrastructure Architecture design principles as describes in the *Infrastructure Architecture - Standards and technical guidelines*

7.2.5. Public institutions shall develop *ICT Acceptable Use rules* to ensure that they understand what is considered acceptable and unacceptable in use of the ICT resources and hence ensure how individuals within their organisations should adhere to the rules for usage of ICT facilities and data as described in the Institutional ICT Policy (rules) as describes in the *Infrastructure Architecture - Standards and technical guidelines*

7.2.6. Public Institutions shall develop the *ICT Acquisition, development and maintenance guideline* to ensure mitigation of silos procurement, vendor lock in and cost optimization throughout ICT lifecycle as describes in the *Infrastructure Architecture - Standards and technical guidelines*

7.2.7. Public Institutions shall adhere to the procurement processes for the acquisition, development and maintenance of all ICT equipment and software.

7.2.8. Public instructions shall adhere to server infrastructure standards as describes in the *Infrastructure Architecture - Standards and technical guidelines*

7.2.9. Public Institutions shall leverage on existing e-government initiatives such as Government Network (GOVNET), Government Mailing Systems (GMS), Government Data Centre (GDC) and Government Mobile Platforms.

7.2.10. Public Institution shall have knowledgeable and appropriately skilled human resources accountable for its on-going ICT operations, management, maintenance, maturity and evolution. *Appendix – Illustration No. 1 ICT Organisation Capability* provides the generic list of required ICT capabilities in a Public Institution.

7.2.11. Public Institutions shall be able to recover transactions and data by establishing an effective for Business Continuity Planning (BCP) and Disaster Recovery (DR) as described in the *Infrastructure Architecture - Standards and technical guidelines*

7.2.12. Public Institutions shall refer to Infrastructure Architecture Technical Guidelines as describes in the *Infrastructure Architecture - Standards and technical guidelines.*

7.3. General requirements for consideration on the use of Government Network and Internet:

7.3.1. The Government's aim is to have a single source of internet services for its official use in order to control the usage of the service. When the Government office is procuring the internet service through contractors, the procuring office shall ensure that the contractor is vetted according to the National Security Act No 3 of 1970 and regulations of Government Security of 1999.

7.3.2. Public Institutions shall educate its employees on the safe use of internet services.

7.3.3. The use of internet services should be aimed at increasing productivity in Government's operations. However, the private use of internet services by employees should be either before or after business hours.

7.3.4. Government Employees are not permitted to use Government's internet services to visit unethical sites.

7.3.5. Computers used to prepare and store confidential documents should not be connected to the internet.

7.4. General requirements for consideration on maintenance of ICT equipment:

7.4.1. The government's aim is to ensure that it has sufficient technicians who maintain ICT equipment. It is the responsibility of ICT technicians within the Government to carry out the preliminary maintenance of the ICT equipment within own institutions.

7.4.2. To enable the ICT technicians to carry out this task, each public institution must have a technical tool box with equipment required for basic computer maintenance.

7.4.3. If further maintenance is required, the ICT technical officer should contact the approved contractor for further assistance.

7.4.4. It is prohibited to take the ICT equipment outside the Government offices for maintenance. If there is need for the computer to be taken outside the Government office, then the hard disk drive must be removed from the computer and stored appropriately.

7.4.5. Government ICT officers must keep a service maintenance log book for ICT equipment that will be used as reference for future decisions as instructed in Public Service circular No 5, 2009.

7.5. General requirement for consideration on verification of ICT equipment:

7.5.1. The Government's aim is to have an electronic register of ICT equipment. In the transition period each public institution must have an ICT equipment registry as shown on the appendix A of the Public

Service circular No 5, 2009. Therefore, Government institutions are required to hold correct information of its ICT equipment.

7.6. General requirements for consideration on the use of mobile data storage:

7.6.1. The Correct Use of Mobile Data Storage Device :-

a. Public servants should be educated regarding the safe use of ICT before commence using the devices.
b. Public servants must use the mobile data storage devices only on Government work. However, it is not permitted to mix official information and private information in the same device.
c. Public documents on transit via flash disk, portable hard drives, phones, iPOD etc must be deleted from these devices once the transfer process is completed.
d. Public servants must not use CD ROM, DVD, and back up tapes for unintentional transfer or storage of information for future uses.
e. Public offices when procure mobile data storage devices must adhere to the directives from the President's Office, Public Service Management.

7.6.2. Registration of Mobile Data Storage Devices:-

a. Mobile Data storage devices should be registered in institution's ICT asset registry with the user information as directed by Public Service circular No 5 of the year 2009.
b. Transfer of mobile data storage devices must adhere to the regulations guiding the issuing of office equipment.

7.6.3. Storage/Sage Keeping of Mobile Data Storage:-

a. Mobile data storage devices must be stored in the Government Offices by the Government's guides for safe keeping of information and equipment. If a public servant requires to take the storage devices outside the Government Office he/she must inform the authorised person.
b. When the mobile data storage device is lost, the loss must be reported to the authority immediately for necessary actions to be taken.

7.6.4. Destruction/Decommissioning of Mobile Data Storage Devices:-

a. When the use of mobile data storage device (when the device becomes obsolete), the device must be sent to the Directorate of Records and Archives Management (DRAM) for destruction.
b. It is forbidden to sell, issue as a gift, or to switch the ownership of Government's mobile data storage devices.

7.7. General requirements for consideration on registration of Government Email Address

7.7.1. Every public institution will be required to have email addresses with the following format:

a. The ministries, departments, authorities, agencies, regional administrative and municipal councils will use ".go.tz".
b. High education institutions will use "ac.tz".
c. Public education institutions will use "edu.tz".

7.7.2. There will be 3 types of Government email addresses as follows:

a. Institutional address: This will be used for all institution's communications and its format will be as follows – name@institution_name followed by "xx.tz".
b. The email address for the department or section will have the following format – department_name@institution_name.xx.tz.

This address will be for the department and sections heads.

Institution/Department/Section email addresses for internal communication in groups (group mail and mailing list)
These will be as follows: staff@institution_name.xx.tz
This is important for all staff: staff@institution_name.xx.tz

IMPORTANT: Email is the simplest way to send message directly to many people at once. But the following precautions should be taken:

a. Group emails should only be sent to staff who are relevant to the information
b. Email administrators should ensure that group emails cannot receive messages from email addresses outside the institution.

7.8. General requirements for consideration on the use of Government Email Address

i. Government email addresses should only be used for Government communication only.
ii. Personal email addresses eg yahoo.com. Hotmail.com etc should not be used for Government communication. Where the public institution is not able to own official email addresses, the institution should contact eGA to acquire a single email address that will be used for communication (sending and receiving Government information).
iii. In no circumstances the public servant is prohibited to send of distribute forward messages by using the Government email address.
iv. Public servants are required to delete unimportant emails or old emails to reduce storage space usage in email servers.

v. Email communications from the Government Offices to the external institutions should follow the communication protocol as stated in section B3 – B14 in the Standing Order, 2009.

vi. When the public servant sends an official email communication outside the institution, the copy should be made to the institution's Accounting Officer or whoever is acting as the Accounting Officer.

vii. The Government ICT officers should offer regular trainings on good and correct use of emails to the public servants.

viii. Public servants are not allowed to distribute information that is against public service ethics as illustrated in the Public Service Ethics Regulations section No 9.

7.9. Public Institutions shall take the following important matters into consideration:

7.9.1. Avoid allowing non-government employees to use Government ICT equipment or public servant to use Government ICT equipment for personal gains unless to improve knowledge and productivity of the said institution.

7.9.2. Government computers must have passwords and every user must ensure his/her computer is under password control when away from it for more than 30 minutes or else it should be switched off.

7.9.3. In the circumstances that the public institution has LAN, then the network should encourage sharing of information and equipment (ie printers, scanners etc.) to reduce costs and increase productivity.

7.9.4. It is prohibited to sell Government's used computers with their data storage device (devices must be removed).

7.9.5. Hard disk drives that are damaged and not reparable or its computers have been put on sale, should be surrendered to the Department of Records and Archiving Management.

7.9.6. Before procuring ICT equipment, the public institution must acquire specifications/standards from PO-PSM.

i. ICT students who are on field training in Government offices should be closely supervised by ICT officers in the institution.

ii. Every Government office must have ICT section that reports directly to the Accounting Officer as determined by the Presidential Implementation Committee, 2006.

iii. Following establishment of eGA, when public institutions require technical assistance in ICT they should contact the e-Government Agency.

8. ICT Security Architecture Guidelines

8.1. Current Situation

The Security Architecture provides guidance on how Public Institutions will securely and economically protect their business including access to information, compliance with regulatory requirements to ensure integrity, confidentiality and availability of information. The Government

has undertaken several initiatives to implement information security including the establishment of Tanzania Computer Emergency Response Team (TZ-CERT) to ensure high and effective level of network and information security within the country. There are challenges such as inadequate framework for information security management, insufficient resources committed for information security and limited awareness of security rules in the Government.

8.2. Security Architecture Consideration

8.2.1. Public Institutions shall implement security mechanism for keeping data protected from unauthorized access so as to ensure data privacy while maintaining data confidentiality.

8.2.2. Public Institutions shall implement security measures built into their applications to minimize the likelihood of information manipulation, unauthorised access, theft, modification, or deletion of sensitive data.

8.2.3. Public Institutions shall implement adequate security mechanisms for network appliances, local/remote access control, authentication, firewall protection, network intrusion detections, and security administration.

8.2.4. Public Institutions shall implement server access control, host intrusion detections, use of server and desktop based anti-virus, anti-spyware, software patch management, storage security, IP security, communications endpoint security etc.

8.2.5. Public Institutions shall adopt, enforce and monitor user internet usage rules, authentication mechanisms for verification of user identify such as two-factor authentication, biometrics based authentication, increase security awareness among users and employees and conduct security training.

8.2.6. Public Institutions shall adhere to standards and technical guidelines associated to physical security. This includes security characteristics concerned with restricting physical access by unauthorized personnel (potential intruders) to controlled facilities (buildings, computer rooms, data centres etc.) along with the access systems and types of access controls used in those same facilities or sites.

8.2.7. Public Institutions shall adhere to ICT security Technical Guidelines the *Security Architecture - Standards and technical guidelines* and consult with eGA for further guidance.

8.3. Information Security Governance and Management

8.3.1. Public institutions shall develop Institutional general ICT Security rules. These are high level directives giving instructions on how ICT Security in the respective Institution can be managed. Public Institutions should make reference to the standards on the creation of

General ICT Security Rules as described in the ICT Security Architecture Technical Standards.

8.3.2. Public institutions shall implement ICT Security Governance provisions to provide direction and oversight to their General ICT Security Rules.

8.4. ICT Security Operations

8.4.1. Public Intuitions shall ensure that processes, technologies and facilities are in place to support the management of information systems while in production

8.5. ICT Asset Management

8.5.1. Public Institutions shall identify, classify and manage their ICT assets such as network, systems, application, storage and data.

8.6. Identity and Access Management

8.6.1. Public Institutions shall ensure that access to information systems and information assets is controlled.

8.7. ICT Security Incident Management

8.7.1. Public Institutions shall ensure Information Security-related incidents are identified, contained, managed and recovered from in a timely and effective manner.

8.8. Information Systems Continuity Management

8.8.1. Public institutions shall develop Institutional Disaster Recovery plan by referring the ICT Disaster Recovery template as described in the ICT Security Architecture Technical Standards.

8.9. Information Systems Acquisition, Development and Maintenance

8.9.1. Public Intuitions shall ensure that information systems and Information Security controls are designed, developed, implemented and tested in a manner aligned to achieve defined, specific Information Security requirements.

8.9.2. Public Institutions shall ensure that goals and initiatives of the Institutions' ICT Security strategy are adhered during engagement with third-parties.

8.10. Human Resources Security

8.10.1. Before access is granted to Government information assets, Public Institutions shall ensure that personnel have been screened by appropriate authorities.

8.10.2. Institutions shall ensure that personnel have the required information, training, skills, awareness and competencies to process Government information in a manner appropriate to the information's classification.

8.11. Physical and Environmental Security

8.11.1. Public Institutions shall provide protection to facilities used in the creation and management of information assets. The protections deployed shall:

i. Ensure critical or sensitive information processing facilities are physically protected from unauthorized access, damage, and interference; and

ii. Equipment will be protected from physical and environmental threats.

8.12. Compliance and Audit

Public Institutions shall ensure that findings of internal and external audits relating to ICT Security are worked on.

9. Process and Governance

9.1. Current Situation

Process and governance is the set of mechanisms through which ICT projects are driven from national level and implemented at a public institution level. It provides a mechanism for defining, implementing, managing and measuring the effectiveness of the above 8 architecture segments defined in the previous sections. Currently there is a lack of coordination and ICT project governance amongst Public Institutions when it comes to implementation of ICT initiatives, which in turn results in duplication of ICT projects across the government.

9.2. Process and Governance Considerations

9.2.1. Public Institutions shall consider the Governance Framework defined below for the purpose of effective planning, implementation and monitoring of the e-Government related standards and guidelines. The Governance Framework consists of 3 core tiers namely:

i. E-Government Standards and Guidelines Advisory Committee - the leading authority in charge of endorsement, enforcement and approval of the e-government related standards and guidelines.

ii. Government Project Team (GPT) – for overseeing the implementation of the proposed standards and guidelines in Public Institutions.

iii. E-Government Working groups – the drivers who should support the actual work of developing and managing the e-government related standards and guidelines for each of the above architecture segment defined.

9.2.2. The ICT Head of Section, Unit or Department shall be responsible for ensuring that the recommended e-government standards and guidelines are incorporated in the design of the proposed ICT/ e-Government initiatives.

9.2.3. The ICT Head of Section, Unit or Department shall work in close collaboration with the e-Government Working Groups and GPT for programme and portfolio management.

9.2.4. Public Institutions shall consult eGA for any future e-government initiatives.

9.2.5. Public Institutions must prepare a report after conducting self-assessment on their ICT/e-Government initiatives to assess levels of compliance by making use of the checklists provided and submit copy of the report to eGA for further guidance.

9.2.6. Public Institutions shall be audited to assess compliance of ICT/ e-government initiatives through monitoring and audit mechanisms.

9.2.7. Public Institutions shall seek consultation from eGA in the event of changes in technology and new developments in their operations that may impact the e-government related standards and guidelines.

9.2.8. Public Institutions shall refer to the *Process and Governance for Enterprise Architecture Ref No: eGA/EXT/ARC/009* and consult with eGA for further guidance.