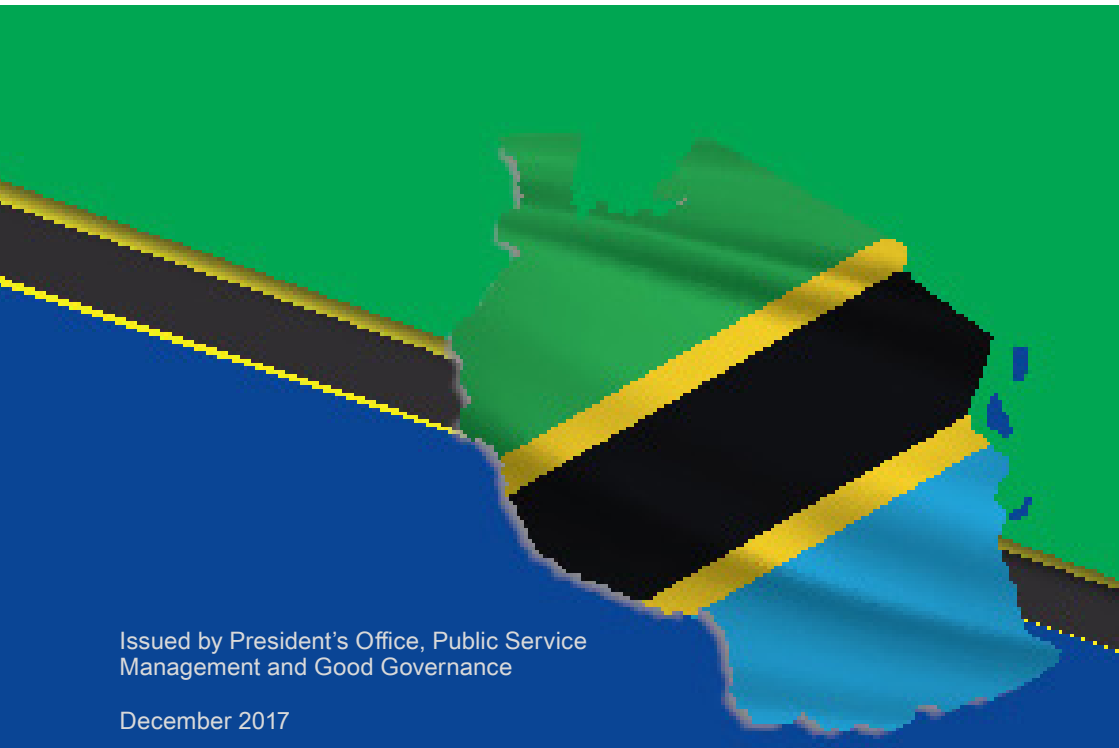
THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE,
PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

E-GOVERNMENT GUIDELINES



Issued by President's Office, Public Service Management and Good Governance

December 2017

THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE,
PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

E-Government Guidelines

Table of Contents

GLOSSARY

Term	Definition
Architecture	The structure of components, their inter-relationships and the principles and guidelines governing their design and evolution over time.
Disaster Recovery Plan	In the context of ICT, this is a documented process or set of procedures to recover and protect ICT business resources in the event of a disaster. It describes how an organization is to deal with potential disasters without losing data/information.
eGA	Institution Responsible for e-Government Policy Implementations.
Enterprise Architecture (EA)	Enterprise Architecture (EA) is the logical organization of a business and its supporting data, applications and IT infrastructure, with clearly defined goals and objectives for the future success of the business.
Interoperability	The ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged.
Open standard	A standard that is publicly available and has various rights to use associated with it and may also have various properties of how it was designed.
Proprietary standard	Privately owned standard widely emulated or followed in an industry due to its owner's market power, but not officially approved by an independent standards body such as ISO.
Service Delivery Platform	System architecture/environment enabling efficient creation, deployment, execution, orchestration and management of one/more service classes
Whole of Government (WoG)	Refers to Public Institutions working across organizational boundaries to achieve a shared goal and an integrated government response to particular issues. Approaches can be formal and informal. They can focus on policy development, program management and service delivery.

FOREWORD

The Government of Tanzania has effected a number of public sector reforms with the objective of improving delivery of services to the public. Part of these reforms include the decision by the Government to leverage Information and Communication Technology (ICT) to improve Government business processes and service delivery. The primary purpose of adopting ICT was to ensure that the public sector is able to deliver quality, effective and efficient services to its citizens. Over the years, the deployment of ICT by Public Institutions to meet the expected results, has been a challenge. To address the challenges, the Government issued Staff Circular No. 5 of 2009, followed by the 2012 Guidelines that were meant to guide the effective and safe use of ICT equipment and systems across Government.

In spite of these efforts, the adoption of ICT in the public sector remains incoherent due to the fact that they are not anchored in Institutional Strategic Plans leading to, absence or little value realized from ICT investment; fragmented e-Government systems that are not integrated and hence cannot share information and duplicated e-Government initiatives and systems. To correct this, the Government undertakes to set Standards and Guidelines that will ensure ICT is properly governed, planned, implemented and used in all Public Institutions for improved service delivery.

These e-Government Guidelines are therefore intended to take Whole of Government (WoG) approach for the adoption of **ICT in Public Institutions. The Guidelines are categorized into six e-Government Focus Areas; ICT Policy, ICT Strategy, Enterprise Architecture, Security Architecture, ICT Governance and General Requirements for Compliance.** Each of these areas provides directives, standards and important matters that must be considered by all Public Institutions, ICT Experts and Public Servants in the use of ICT.

I believe that the use of these Guidelines will reduce duplication and eliminate fragmented and inconsistent approaches to ICT. The WoG approach to ICT will lead to cost effective investment in ICT, improved efficiency and coordination in service delivery. Finally, it is intended that these Guidelines as well as other e-Government Technical Standards that are in use will be effectively used by all Public Institutions to bring positive change and contribute to the attainment of social and economic benefits to the people of Tanzania.

Hon. George Huruma Mkuchika (MP)

MINISTER OF STATE, PRESIDENT'S OFFICE PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

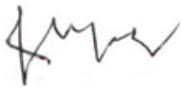
STATEMENT OF THE PERMANENT SECRETARY

The Government of Tanzania developed and adopted the National e-Government Strategy in 2009 and revised in 2013, to allow for a more coordinated and citizen-driven e-Government initiative. The Strategy aimed to leverage the full potential of ICT to achieve good governance and proper social and economic development by establishing effective e-Government service delivery platforms.

The implementation of the Strategy has attained several achievements and lessons learned that benefit redress in development of these guidelines. It was generally appreciated that Public Institutions would be better placed to implement the Strategy using clear directives in the form of standards and guidelines. The Government has thus developed the guidelines as well as e-Government Technical Standards to ensure that Public Institutions appropriately plan, design, acquire, implement and manage Government services and delivery using ICT.

The Government thus directs all Public Institutions including Ministries, Independent Departments, Regional Secretariats, Local Government Authorities, Government Agencies/Authorities, Parastatal Organizations, Public Corporations and other Government autonomous or semi-autonomous institutions to adhere to these Guidelines and associated Technical Standards provided for in this document. The Technical Standards will be regularly updated and published based on technological changes, business needs and requirement of the Government. The Ministry responsible for e-Government will regularly monitor implementation of ICT use across Government.

Guidelines on Effective and Safe Use of ICT Equipment and Systems in the Government ***("Mwongozo wa Matumizi Bora, Sahihi na Salama ya Vifaa na Mifumo ya Teknolojia ya Habari na Mawasiliano")*** of 2012, are hereby revoked.



Dr. Laurean Josephat Ndumbaro
PERMANENT SECRETARY (ESTABLISHMENT

I. INTRODUCTION

a. This Document comprises detailed guidelines that provide directives in various aspects of e-Government implementation; starting from inception to delivery as shared or addressed to individual institution's core processes. The Guidelines are aimed at improving Government operations that ultimately result into improved public service delivery. To implement the Guidelines, practitioners in Public Institutions should read them together with Technical Standards that are referenced in various sections of the Document. The Technical Standards provide frameworks for institutions to implement directives provided in the Guidelines.

b. The Document has six (6) Sections; each with a specific theme, directives, instructions, standards and guidelines for planning, design, acquisition, implementation, management and use of e-Government solutions. The first section is on ICT Policy Guidelines which direct Public Institutions to develop and operationalize Institutional ICT policies. It provides guidelines for compliance, acceptable and secure use of ICT by Public Institutions, employees and external stakeholders.

c. The Second Section are the ICT Strategy Guidelines which direct Public Institutions to establish and implement the ICT strategy. The strategy will help Institutions to invest in ICT solutions that are aligned to their strategic objectives in order to ensure value for money ICT investments.

d. The Third Section outlines the Enterprise Architecture (EA) Guidelines. The EA Guidelines direct Public Institutions to adopt EA as an approach to implementing e-Government services. EA identifies all the main components of an Institution; its Business Processes, Information Systems and Infrastructure; the ways in which the components work together to achieve defined business objectives and the way in which the information systems support the business processes of the Institution. In adhering to EA, the Government will reduce risk of fragmented and duplication of efforts and hence achieve greater interoperability.

e. The Fourth Section presents Security Architecture Guidelines. The Security Architecture Guidelines direct Public Institutions to adopt security architecture as an approach to designing and implementing information security infrastructure. It provides the framework to protect Institutional Business Processes and information resources, enable secure communication, and ensure that new methods for delivering services are secure.

f. The Fifth Section elaborates e-Government Governance and Management Guidelines. The e-Government Governance and Management Guideline directs Public Institutions to establish ICT governance and management structures and processes needed to oversee and manage the investment and appropriate use of ICT in the institution. It provides the framework that describes institutional structures required to effectively leverage ICTs in Government, high level processes to be put in place to overcome departmental silos, development of capacity within the Government focusing on innovations and management of transformational change.

g. The Last Section of this document provides for General Requirements for Appropriate, Proper and Safe Use of ICT Equipment and Systems.

h. These Guidelines are developed to complement other guides that were issued previously. Therefore Public Institutions shall continue to comply with:

   i. "Mwongozo wa Mawasiliano kwa Njia ya Video Serikalini, Desemba 2014" and amendments made from time to time.

   ii. "Mwongozo wa Kusimamia na Kuendesha Tovuti za Serikali, Desemba 2014" and amendments made from time to time.

   iii. Technical Standards and Guidelines for Government Websites, December 2014 and amendments made from time to time.

   iv. Government e-mail naming standard, 2016. Or any other amendments made from time to time.

   v. Government Domain Naming Standards, 2016 and amendments made from time to time.

   vi. All e-Government Technical Standards issued by the Institution responsible for e-Government implementation.

II. VISION AND PURPOSE OF THESE GUIDELINES

a. E-GOVERNMENT VISION

As stated in the National e-Government Strategy Document (2013), the e-Government Strategic Vision is **"To have an effective and better Government that provides innovative public service delivery enabled by ICT".**

b. PURPOSE OF THESE GUIDELINES

The purpose of these Guidelines is to provide guidance to Public Institutions on how to leverage ICT in improving service delivery. This guideline document is intended for use by all Public Institutions including Ministries, Independent Departments, Regional Secretariats, Local Government Authorities, Government Agencies/Authorities, Parastatal Organizations, Public Corporations and Government autonomous or semi-autonomous institutions.

SECTION ONE: ICT POLICY GUIDELINES

1.1. ICT and Socio-Economic Development

1.1.1. ICT like other technologies before it, is adopted to galvanize productivity and ultimately to contribute to achieving socio-economic development across the world. However, the manner in which ICT is acquired, managed and used is critical to the attainment of organisational costs. In this Section of the Guidelines, the need for ICT Policy is emphasised

1.1.2. ICT policy provides a set of principles intended to govern the acquisition, implementation, adoption, management and use of ICTs in organizations. It forms the philosophy and basis to underpin the planning and development and utilization of ICTs in a particular setting.

1.2. Current Situation

1.2.1. Some Public Institutions have developed and operationalized institutional ICT policies. However, a large number of Institutions have yet to establish and adopt institutional ICT policies. The absence of a policy on ICT implies that the acquisition, management and use of ICT may not be properly governed. This may have, to a large extent, contributed to inefficient and improper use of ICT in some of those Institutions.

1.2.2. The purpose of these Guidelines is to direct Public Institutions to put in place ICT policy. In this regard the Government is providing Technical Standards as a guide to formulating institutional ICT policy.

1.3. Institutional ICT Policy Development Guidelines

In order to effectively leverage ICT, Public Institutions shall abide by the following principles:

1.3.1. Develop and implement institutional *ICT Policy* to provide directives for appropriate planning, acquisition, adoption, implementation, management and use of ICT in accordance with *ICT Policy - Technical*

Standards.

1.3.2. The *ICT Policy* should provide directives to:

i. Ensure corporate ICT strategies are prepared, endorsed and periodically reviewed and updated, in order to be closely aligned to the organization's business needs and priorities and yield value for ICT investment, as directed in Section 2.3;

ii. Adopt Enterprise Architecture as an approach to implementing e-Government services to ensure efficient and effective transformation efforts, as directed in Section 3.4;

iii. Ensure Security Architecture is prepared, endorsed, implemented and periodically reviewed and updated, in order to enable secure, efficient transaction of business and delivery of services, as directed in Section 4.3;

iv. Ensure the definition, establishment, and management of a framework for the ICT Governance, ICT Service Management, Enterprise Architecture Governance, and ICT Project Management are in alignment with the Mission, Vision and Values of their Institution, as directed in Section 5.3.

1.3.3. Update the ICT Policy based on changes in business and processes to reflect both, the internal and external environment.

SECTION TWO: ICT STRATEGY GUIDELINES

2.1. How ICT Strategy Can Lead to Results

2.1.1. The Strategy entails formulation, deployment and maintenance of ICT initiatives in Public Institutions and encompasses aspects that require intelligent planning. A comprehensive ICT Strategy is therefore essential for effective implementation of the ICT initiatives.

2.1.2. ICT Strategy defines the Institution's long-term ICT goals and the best approaches for achieving those goals to support its current and future business needs. The strategy helps Institutions to invest in ICT solutions that are aligned with institutional strategic objectives and avoid investing under vendor/supplier/ donors influence and thus reduce unnecessary costs.

2.2. Current Situation

2.2.1. While there is increased ICT investment and adoption in the Public Sector, most Public Institutions do not have a comprehensive ICT Strategy. The absence of a Strategy means that investment decisions on ICT can be inconsistent and may benefit only one part of the Institution. Such inconsistency can cause Public Institution inefficiency and frustrate processes and services; thereby ICT becoming an obstacle to the achievement of the Institutional goals.

2.2.2. The purpose of this Guideline is to direct Public Institutions to develop and implement institutional ICT Strategies. In this regard, the Government is providing technical standards as a guide to formulating the ICT Strategy.

2.3. Institutional ICT Strategy Development Guidelines

All Public Institutions shall:

2.3.1. Prepare and operationalize an Institutional ICT Strategy to set out a clear focus on using ICT for better service delivery and achieving better value for ICT investment by complying with the *ICT Strategy-*

Technical Standards.

2.3.2. Ensure that ICT Strategic planning engages the Institutional executive leadership.

2.3.3. Ensure that all planning for ICT development and use is being aligned with and serves the Institution's strategic goals and directions.

2.3.4. Ensure that the ICT strategic planning process is carried out by the committees as proposed in the governance structures in Section 5.3 of these Guidelines.

2.3.5. Ensure that each ICT initiative that is expected to be implemented in the institution is included in the ICT Strategy and/or is aligned to the National e-Government Strategy.

2.3.6. Update the ICT Strategy based on changes in business internal and external environments.

SECTION THREE: ENTERPRISE ARCHITECTURE DEVELOPMENT GUIDELINES

3.1. Why Enterprise Architecture?

3.1.1. At policy level, the Government is committed to the improvement of service delivery to the public through e-Governance. While the e-Government Mission is to transform Government operations by leveraging ICT, it is important to recognise that Governments are large organizations characterized by complex structures where individual Public Institutions sometimes work in their respective jurisdictions. This often leads to fragmented business processes and duplicated e-Government systems and technologies that can create obstacles in cross agency interoperability. In order to drive these transformations, the Government need to have a complete understanding of what it is to be transformed and what effect those changes will have. Enterprise Architecture (EA) is a widely used approach to plan and implement efficient and effective transformation efforts.

3.2. What is an Enterprise Architecture

3.2.1. **Enterprise Architecture** is a logical organization of a business process and its supporting data, applications and IT infrastructure, with clearly defined goals and objectives for the future success of the business. A typical architecture consists of diagrams or models, that show how aspects of institutions' business processes relate. In practice, business processes should have an "as-is" architecture that represents its current state, and a planned architecture "to-be" to show the direction of the business over the next one to five years.

3.2.2. In this regard, the Government of Tanzania has decided to adopt EA as the framework to guide the implementation of e-Government initiatives in Government. The adoption of EA approach to developing e-Government capabilities allows the Government to:

(a). Leverage what currently exists in the Tanzanian e-Government landscape across Institutions and Government as a whole;

(b). Understand current business processes "as-is", identify gaps and determine new business processes "to-be" and how to fit them

in existing structures;

(c). Define information structures to fit current needs and to support anticipated ones; and

(d). Demonstrate how technology and resource constraints dictate both what is feasible and the path forward.

3.3. Current Situation

3.3.1. Currently the focus of several e-Government initiatives in Public Institutions is on automating internal operations, with no precedent business process re-engineering efforts. On the same note, the focus of most of these initiatives is largely limited to specific Ministries and Agencies. Despite coordination efforts through eGA, there are still initiatives in some Public Institutions that lack the cross-agency/ministry viewpoint. This creates challenges in taking a Whole-of-Government approach, as a result the e-Government initiative landscape is characterized by fragmented e-Government solutions which are not interoperable and that they cannot interact and share or exchange information.

3.3.2. Another shortcoming is the lack of clear alignment between Government strategy, priorities and e-Government projects implemented at all levels of the Government. As a result, some of the e-Government projects in several Institutions have been implemented on supply driven approach which may not well address business needs compared to demand driven approach.

3.3.3. The purpose of these Guidelines is to direct Public Institutions to adopt EA as an approach to implementing e-Government services. In order to realize WoG through EA, the Government is providing technical standards as a common language to developing and implementing institutional Enterprise Architecture.

3.4. Institutional Enterprise Architecture Development Guidelines

Because of the shortcomings indicated to in section 3.3, Public Institutions shall:

3.4.1. Develop and implement their EA to enable and accelerate the

development of effective Digital Government within the Institution by complying with the *e-Government Enterprise Architecture - Technical Standards.*

3.4.2. When developing their EA, to adhere to interoperability standards as defined in *e-Government Interoperability Framework - Technical Standards* of defining data, application and infrastructure standards.

3.4.3. Develop, as deemed necessary, sectoral/institutional specific interoperability standards that are not covered by the e-Government Interoperability Frameworks (e-GIF).

3.4.4. Use Government designed service driven integration platform to exchange information across all institutions. However, an Institution or a Sector may require institutional/sector level integration platform to facilitate information exchange within an Institution/Sector. In this case an institution responsible for e-Government should be consulted for compliance and approval.

3.4.5. 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 implementation, upgrade of older systems and when reviewing their ICT strategy.

3.4.6. Adhere with e-GIF in their Bidding/Request for Proposal process for any technology product/service intended to be put for use to serve citizens.

3.4.7. Establish their ICT acquisition process in such a way that no ICT investment should be made without an approved architecture and compliance to e-GIF. Therefore Institutions responsible for coordination, oversight and promotion of e-Government implementation should be consulted for compliance and approval.

3.4.8. Consult the Institution responsible for e-Government implementation in the event of changes in technology and new developments in their operations that may affect interoperability.

SECTION FOUR: E-GOVERNMENT SECURITY ARCHITECTURE GUIDELINES

4.1. Effective e-Government Security Architecture

4.1.1. The information, application, and infrastructure layers of EA are all vulnerable to attack by both internal and external threats. The Security Architecture is therefore a unified security design specification for addressing these security challenges, while pursuing the Government's mission of quality service to its Citizens. Security Architecture is an integral and critical component within the EA designed specifically to:

(a). Enable secure, efficient transaction of business and delivery of services;

(b). Enable secure communications and appropriate protection of information resources within all Public Institutions (of Tanzania);

c). Support legal information security requirements established by the Government pertaining to information confidentiality, accessibility, availability and integrity;

(d). Leverage opportunities to obtain IT security synergies and economies of scale.

4.2. Current Situation

4.2.1. Currently information security in most of the Public Institutions is not uniformly implemented. Only few Public Institutions have information security strategies or policies. In Public Institutions with information security mechanisms, these have been built into individual e-Government systems. Security requirements for e-Government can only be fully addressed by taking a holistic approach, i.e. from a strategic perspective, down to operational policies and processes.

4.2.2. The purpose of this Guideline is to direct Public Institutions to adopt Security Architecture as an approach to designing and implementing information security infrastructure. In this regard, the Government is providing technical standards as a common framework for developing and implementing institutional Security Architecture.

4.3. Institutional Security Architecture Development Guidelines

In order to strengthen e-Government Security Architecture, Public Institutions shall:

4.3.1. Perform a business driven risk assessment to evaluate the business influence of vital business assets, likelihoods, effects of vulnerabilities and security threats.

4.3.2. Develop and implement Institutional ICT Security Policy that provides directives for managing ICT Security in the respective Institution by complying with the e-Government Security Policy - Technical Standards.

4.3.3. Develop Disaster Recovery Plan, as part of the ICT Security Policy implementation

4.3.4. Develop Institutional Security Architecture to ensure integrity, confidentiality and availability of information by complying with the *e-Government Security Architecture - Technical Standards.*

4.3.5. Implement, operate and control security mechanisms, services and processes to ensure that the security policy and standards, security architecture decisions, and risk management are mirrored in the real runtime implementation.

4.3.6. Update the Security Architecture as various Institutional plans and policies are changed, technology changes and new risks are discovered and improvements are made to the architectural structure.

4.3.7. When developing their Security Architecture, adhere with interoperability standards as defined in e-Government Interoperability Framework Technical Standards to define data, application and infrastructure standards.

4.3.8. Develop, whenever necessary, their sectoral/institutional specific security standards which are not covered by the *e-Government Interoperability Framework Technical Standards.* Use of open standards shall be given preference over proprietary standards wherever appropriate.

SECTION FIVE: E-GOVERNMENT GOVERNANCE AND MANAGEMENT GUIDELINES

5.1. E-Governance Management

5.1.1. Governance is the most important factor in generating value from ICT and a critical success factor for e-Government initiatives. It is an integral part of corporate governance which consists of leadership, structures and processes to ensure that an organization's ICT sustains the organization's strategies and objectives. In the Public Service, ICT governance entails political and executive leadership, structures and processes that aim at promoting and sustaining ICT use in the Public Sector.

5.1.2. ICT Governance in Public Service should be well instituted in the organizational structure and processes in order to facilitate public and external stakeholders to receive appropriate e-services. In doing so, Public Institutions will be able to effectively manage ICT services, typically in a coordinated manner and not be monopolized by its ICT Division/Unit/Department.

5.2. Current Situation

5.2.1. Currently most of the setup in Public Institutions do not have well defined ICT Governance practices, organizational structure and professional expertise. For example, only few Ministries have formal ICT Departments headed by a Director while most of the Public Institutions have relatively small ICT units headed by a Principal Computer Systems Analyst who reports to the Accounting Officer and performs technical roles rather than playing strategic or management roles. Furthermore, some Public Institutions do not have independent ICT Units and are instead embedded in other administration, planning, statistics Departments.

5.2.2. The purpose of this Guideline is to ensure that Public Institutions establish ICT governance and management structures and processes needed to oversee and manage the investment and appropriate use of ICT. In this regard the Government is providing technical standards to guide the formulation and implementation of the required institutional

ICT governance and management structures and processes. The Standards shall guide institutions to define and implement structures and processes for ICT governance, ICT Security Governance, EA Governance, ICT Service Management and ICT Project Management. The Standard shall also provide a common framework for establishing appropriate ICT Division/Department/Unit to perform ICT Service management functions within Public Institutions.

5.3. Governance and Management Guidelines

Public Institutions shall:

5.3.1. Establish an ICT governance structure and processes to govern and control the implementation and proper use of ICT in the institution by complying with the *e-Government Governance and Management – Technical Standards.*

5.3.2. Establish an *ICT Department/Directorate/Unit that reports directly to the Accounting Officer* by complying with the *e-Government Governance and Management – Technical Standards.*

5.3.3. Ensure that, *ICT Department/Directorate/Section/Unit, works in close collaboration with* the Institution responsible for e-Government implementation, for ICT programme and portfolio management.

5.3.4. Establish ICT security governance structures and processes to oversee the implementation of the required information security by complying with the *e-Government Governance and Management – Technical Standards.*

5.3.5. Establish EA governance structures and processes to oversee the development and implementation of institutional EA by complying with the *e-Government Governance and Management – Technical Standards.*

5.3.6. Implement the ICT service management to ensure effective ICT service delivery and support by complying with the *e-Government Governance and Management – Technical Standards.*

5.3.7. Ensure that e-Government projects are managed in compliance with

the *e-Government Governance and Management – Technical Standards.*

5.3.8. Ensure that e-Government Technical Standards are incorporated in the design of any proposed ICT/ e-Government initiative.

5.3.9. Conduct self-assessment annually on ICT/e-Government initiatives by using assessment tools and submit copy of the report to the Institution responsible for e-Government implementation for notification.

5.3.10. Be audited/reviewed to assess compliance with e-Government Technical Standards through monitoring and audit mechanisms.

SECTION SIX: GENERAL REQUIREMENTS FOR COMPLIANCE

This section provides for general requirements for compliance in the use of ICT equipment and systems in the Public Institutions.

6.1. Use of Government Software and ICT Equipment

Public Institutions shall:

6.1.1. Opt to use of Open Source software over proprietary software whenever possible given the fact that Open Source software are flexible, easily customizable and interoperable.

6.1.2. Prohibit non-Government employees to use Government software, applications systems, ICT equipment or any related asset without prior permission.

6.1.3. Prohibit Public Servants to use Government software, applications systems, ICT equipment or any related asset for personal gain or unethical conduct.

6.2. Use of Government Storage and Mobile Devices

Public Institutions shall:

6.2.1. Remove storage devices, of any form, from ICT equipment such as computers, scanners, printers, servers intended to be disposed.

6.2.2. Adhere to the Guideline for Data Storage, Transfer and Archiving while using official storage or mobile devices.

6.2.3. Comply with Circulars and Guidelines issued by the Institution responsible for Records and Archives Management during disposal of storage devices that are damaged and not repairable or removed from ICT equipment that are intended to be disposed.

6.3. Use of Government Internet Services

Public Institutions shall:

6.3.1. Ensure secure source of Internet services for official use.

6.3.2. Prohibit use of Government Internet services to access unethical sites.

6.3.3. Prohibit use of Government Internet services to access and/or download restricted files, video, music, picture or any other related documents.

6.3.4. Educate employees on the safe use of Internet services.

6.3.5. Ensure that Computers used to prepare and store classified (confidential, secret and top secret) documents are not connected to the Internet directly.

6.3.6. Adhere to Technical Standards and Guidelines for Government Websites of December 2014 for designing any Website, Portal or Portlets as will be updated and provided from time to time.

6.4. Use of Government Elecronic Mailing Services

Public Institutions shall:

6.4.1 Ensure that all official communications through e-mail are through reliable Government mailing systems and the use of disposable e-mails shall not be allowed for official communications.

6.4.2 Ensure that email communications from Government Offices to external institutions follow the communication protocol stipulated under Section B3 – B14 of Standing Orders, 2009.

6.4.3 Ensure that transmission of information classified as confidential follow requirements provided in Section C10 of Standing Orders, 2009.

6.4.4 Manage and maintain mailing systems provided that such systems have attained minimum requirements as specified in Government Domain and e-mail Systems Guideline. Where a mailing system does not meet such requirements, the Institution should use Government Mailing System (GMS) as per GMS Operation Procedures.

6.4.5 Adhere to e-mail operation procedures governing management of e-mails as per *Government e-mail Naming Standards, 2016*.

6.5. Maintenance and Repair of ICT Equipment of Government Elecronic Mailing Services

Public Institutions shall:

6.5.1. Acquire ICT equipment specifications from the Institution responsible for e-Government implementation.

6.5.2. Ensure preliminary maintenance of the ICT equipment and repair are carried out by ICT technicians within their institutions.

6.5.3. Prohibit taking ICT equipment outside Government offices for maintenance and repair UNLESS there is a justifiable reason to do

so. Where there is a justified reason to carryout maintenance outside Government offices, the hard drive or any storage accessories therein must be removed from the equipment and stored appropriately.

6.5.4. Ensure that Contractors and consultants who are engaged to provide ICT services shall be vetted according to the National Security Act No 3 of 1970 and Regulations of Government Security of 1999.

Issued by President's Office, Public Service Management and Good Governance

DECEMBER 2017