**THE UNITED REPUBLIC OF TANZANIA**

**PRESIDENT'S OFFICE, PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE**

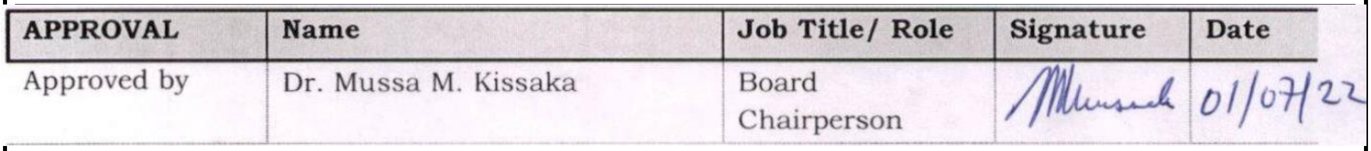
**e-GOVERNMENT AUTHORITY**

## Document Title

Guidelines and Criteria for Cloud and Stand-alone Deployment of e-Government Shared Systems

## Document Number

eGA/EXT/IRA/007



| APPROVAL | Name | Job Title/ Role | Signature | Date |
|---|---|---|---|---|
| Approved by | Dr. Mussa M. Kissaka | Board Chairperson | | 01/07/22 |

# PREFACE

Section 5 (2) (k) and (r) of the e-Government Act requires the e-Government Authority to facilitate Public Institutions to access shared ICT infrastructure and systems as well as establish and maintain secure shared Government ICT infrastructure and systems. However, deployment of either cloud based or stand-alone e-Government Shared Systems by Public Institutions to meet the expected results, has been a challenge due to absence of proper guidelines and criteria that describes important terms to be considered before deployment.

Being the case, the Authority has prepared guidelines and criteria to guide proper, effective and secure deployment of either cloud based or stand-alone e-Government Shared Systems to Public Institutions.

Dr. Mussa M. Kissaka
**BOARD CHAIRPERSON**

## Table of Contents

# 1. INTRODUCTION

## 1.1. Overview

e-Government Authority is a public institution established by e-Government Act No.10 of 2019 with mandate to coordinate, oversee, and promote e-Government initiatives and enforce e-Government related policies, laws, regulations, standards and guidelines to Public Institutions.

## 1.2. Rationale

To provide guidance on proper, effective and secure deployment of either cloud based or stand-alone e-Government shared systems.

## 1.3. Purpose

This document provides the guidelines and criteria for deployment of either cloud-based or stand-alone e-Government shared systems, such as e-office, GMS and etc.

## 1.4. Scope

The guidelines and criteria in this document shall be adhered by public institutions upon deciding whether to deploy cloud-based or stand-alone e-Government shared systems.

# 2. GUIDELINES AND CRITERIA FOR DEPLOYMENT OF e-GOVERNMENT SHARED SYSTEMS

## 2.1. GUIDELINES

### 2.1.1. Cloud-based e-Government Shared Systems

A public institution intending to deploy cloud-based e-Government shared system shall ensure that:

2.1.1.1. File series and keyword list are prepared with assistance, advice and guidance from PO-RAMD.

2.1.1.2. System users are trained to use the systems appropriately.

A public institution intending to offer cloud-based e-Government shared service shall ensure that:

2.1.1.3. Offline Backup is taken regularly, tested and Primary Site (PR) and Disaster Recovery Site (DR) should meet Critical Data Center requirements as described in Data Center Standards for Public Institutions **e-GA/EXT/IRA/003**.

2.1.1.4. Public Institution should continuously monitor hosting systems appropriate for effective capabilities of detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets.

2.1.1.5. Have an SLA specifying roles for respective parties, including client and support.

### 2.1.2. Stand-alone e-Government Shared Systems

A public institution intending to deploy stand-alone e-Government shared system shall ensure that:

2.1.2.1. Hosting environment (server room) should be assessed for security before deploying the systems.

2.1.2.2. File series and keyword list are prepared as per PO-RAMD procedures and guidelines.

2.1.2.3. Offline Backup is taken regularly, tested and Primary Site (PR) and Disaster Recovery Site (DR) should meet Critical Data Center requirements as described in Data Center Standards for Public Institutions – **eGA/EXT/IRA/003** and one of the Disaster Recovery Site (DR) should be in Government approved Data Centres i.e. The National Internet Data Center or Government Data Center.

2.1.2.4. System users are trained to use the systems appropriately.

2.1.2.5. Public Institution should continuously monitor deployed systems appropriate for effective capabilities of detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets.

2.1.2.6. Systems receive effective and Timely Support and maintenance as described by section 2.2.2 of the *Guidelines for development, Acquisition, Operation And maintenance of e-Government Applications - eGA/EXT/APA/006.*

2.1.2.7. The system is always running on latest updated version and any security patches and updates are implemented.

A public institution intending to offer stand-alone e-Government shared service shall ensure that:

2.1.2.8. Have a change management procedure, and have a proper version control which e-GA should be concerned, to ensure availability of latest updated version to all the users whenever required.

2.1.2.9. Have an SLA specifying roles for respective parties, including client and support.

## 2.2. CRITERIA

### 2.2.1. Cloud-based e-Government Shared Systems

A Public Institution to be given access to e-Government Systems in shared infrastructure shall meet the following criteria.

#### 2.2.1.1. Government Institution

The institution requested the deployment of e-Government Shared Systems shall be a Public Institution.

#### 2.2.1.2. Network Infrastructure

The Public Institution must firstly be connected on Government Network (GOVNET) either by POP or MPLS connection or Government approved VPN; this will work for e-Office and other systems.

#### 2.2.1.3. Domain Name

The Public Institution shall first have domain name registered or transferred to e-Government Authority, this will work for GMS.

#### 2.2.1.4. Government Mailing System

The Public Institution shall have GMS before deployment of other shared systems such as e-Office and etc.

### 2.2.2. Stand-alone e-Government Shared Systems

For a Public Institution to deploy stand-alone e-Government Shared Systems shall meet the following criteria.

#### 2.2.2.1. Government Institution

The institution requested the deployment of e-Government Shared Systems shall be a Public Institution.

#### 2.2.2.2. Exceptional Customization of the respective system

The Public Institution will be allowed to deploy stand-alone e-Government Shared Systems if and only if the e-Government Authority verifies the Institutional need for customization of the respective system, and those changes are within the scope of the respective business process of the system, e-Government standards and guidelines.

#### 2.2.2.3. Network Infrastructure

The Public Institution will be allowed to deploy stand-alone e-Government Shared Systems if the Institution cannot be connected on GOVNET and the e-Government Authority have assessed and is satisfied that, for that time it is not possible to connect the Institution on the GOVNET.

#### 2.2.2.4. Internal ICT Team Capacity

The Public Institution will be allowed to deploy stand-alone e-Government Shared Systems if it has adequate capacity of internal ICT team in systems and infrastructure administration.

#### 2.2.2.5. Environmental Deployment Requirements

The Public Institution shall ensure the following are in place before deploying stand-alone e-Government Shared Systems.

i. Hosting environment (Server room) should meet the minimum requirements specifications and technologies that will be provided by the Authority to a Public Institution such as Storage Server, RAM, CPU, OS, Web Server and etc.

ii. Primary (PR) site and Disaster Recovery (DR) site have access for internet for initial installation.

iii. Primary (PR) site and Disaster Recovery (DR) site servers are on place and having same specifications and mounted on respective datacentre and one of the DR site is a government owned datacentre i.e. the National Internet Datacenter or Government Datacenter.

iv. Licenses for hosting environment using any vendor based solution (like hypervisor/OS/Package).

v. Hosting environment meets Critical Data Center requirements in term of hazard, security, power systems, cooling systems and others as described in *Data Center Standards for Public Institutions – eGA/EXT/IRA/003.*

vi. Primary (PR) site and Disaster Recovery (DR) site are on different location as per general Data Center guidelines (preferably different regions).

vii. Primary (PR) site and Disaster Recovery (DR) site are on network which can communicate to each other via specific ports (example SSH 22, Postgres 5432, MySQL 3306).

viii. Authentication method expected should be in place (example DB/Active Directory or any other).

## 3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

This document shall be:

3.1. Effective upon being signed by the e-Government Authority Board chairperson on its first page.

3.2. Subjected to review at least once every three years or whenever necessary changes are needed.

3.3. In case of any exceptions to this document, its application must duly be authorized by the e-Government Authority Board chairperson before documentation.

## 4. GLOSSARY AND ACRONYMS

### 4.1. Glossary

None

### 4.2. Acronyms

| | |
|---|---|
| **DR** | Disaster Recovery Site |
| **e-GA** | e-Government Authority |
| **GMS** | Government Mailing System |
| **GOVNET** | Government Network |
| **ICT** | Information and Communication Technology |
| **MPLS** | Multiprotocol Label Switching |
| **OS** | Operating System |
| **POP** | Point of Presence |
| **PO-RAMD** | President's office Records and Archives management department |
| **PR** | Primary Site |
| **RAM** | Random Access Memory |
| **CPU** | Central Processing Unit |

## 5. RELATED DOCUMENTS

**5.1.** e-Government Security Architecture Standards and Technical guidelines *(eGA/EXT/ISA/001).*

**5.2.** e-Government Infrastructure Architecture Standards and Technical guidelines *(eGA/EXT/IRA/001).*

**5.3.** Data Center Standards for Public Institutions – *(eGA/EXT/IRA/003).*

**5.4.** Guidelines for development, Acquisition, Operation And maintenance of e-Government Applications *( eGA/EXT/APA/006).*

## 6. DOCUMENT CONTROL

| Version | Name | Comment | Date |
|---|---|---|---|
| Ver. 1.0 | e-GA | Creation of Document | July 2022 |

## Appendix I: Checklist for Cloud Based Deployment Requirement

| No. | Category | Key requirements | Remarks (Yes/No) | Requirement Weight (%) |
|---|---|---|---|---|
| 1. | **Government Institution** | The requested Institution is a Government Institution? | | **10** |
| 2. | **Network Infrastructure** | The Public Institution is connected on Government Network (GOVNET) either by POP or MPLS connection?<br>***(This work for e-Office and etc.)*** | | **30** |
| 3. | **Domain Name** | Public Institution's Domain Name is registered or transferred to e-Government Authority?<br>***(This work for GMS)*** | | **30** |
| 4. | **Government Mailing System** | The Public Institution is using GMS to support deployment of other shared systems such as e-Office and etc. | | **30** |

## Appendix II: Checklist for Standalone Deployment Requirement

| No. | Category | Key requirements | Remarks (Yes/No) | Requirement Weight (%) |
|---|---|---|---|---|
| 1. | **Government Institution** | The requested Institution is a Government Institution? | | **10** |
| 2. | **Exceptional Customization of the respective system** | e-Government Authority verified if the Institution needs customization of the respective system, and those changes will affect other Institutions on the shared infrastructure. | | **10** |
| 3. | **Network Infrastructure** | The Public Institution not connected on Government Network (GOVNET) and the e-Government Authority satisfied, for that time it is not possible to connect the Institution on the GOVNET. ***(This work for e-Office and etc.)*** | | **10** |
| 4. | **Internal ICT Team Capacity** | e-Government Authority satisfied with the capacity of internal ICT team for systems administration. | | **30** |
| 5. | **Environmental Deployment Requirements** | Hosting environment met the minimum requirements specifications and technologies provided by the Authority to a Public Institution such as Storage Server, RAM, Processor, OS, Web Server and etc. | | **6** |
| | | Primary (PR) site and Disaster Recovery (DR) site servers are on place and having same specifications and mounted on respective data center. | | **6** |

| No. | Category | Key requirements | Remarks (Yes/No) | Requirement Weight (%) |
|---|---|---|---|---|
| | | There are Licenses for hosting environment using any vendor based solution (like hypervisor/OS/Package). | | **4** |
| | | Hosting environment meets Moderate Critical Data Center requirements in term of hazard, security, power systems, cooling systems and others as described in Data Center Standards for Public Institutions – eGA/EXT/IRA/003. | | **6** |
| | | Primary (PR) site and Disaster Recovery (DR) site are on different location as per general Data Center guidelines (preferably different regions). | | **4** |
| | | Primary (PR) site and Disaster Recovery (DR) site are on network which can communicate to each other via specific ports (example SSH 22, Postgres 5432, MySQL 3306). | | **4** |
| | | Can both Primary (PR) site and Disaster Recovery (DR) site have access for internet for initial installation? | | **4** |
| | | Authentication method expected are in place (example DB/Active Directory or any other). | | **6** |