




THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

Document Title

e-Government Agency Services - Security Responsibilities Guidelines

Document Number

eGA/EXT/BSA/004

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Jabiri Bakari	CEO – eGA		03/07/2019

Version: 1.0 – July 2019

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

Table of Contents

1. OVERVIEW	2
1.1 Introduction	2
1.2 Rationale	3
1.3 Purpose	3
1.4 Scope	3
2. GUIDELINES FOR SECURITY RESPONSIBILITIES	4
2.1. Website Services	5
2.1.1. Website developed by eGA and hosted by eGA	5
2.1.2. Website developed by Public Institution and hosted at eGA	8
2.1.3. Website developed by eGA and not hosted at eGA	10
2.2. Application Services	11
2.2.1. Application developed by eGA and hosted by eGA	11
2.2.2. Application developed by Public Institution and hosted by eGA	12
2.2.3. Application developed by eGA and not hosted at eGA	12
2.3. Website connected with Application	12
2.3.1. Website linked with Application hosted at eGA	13
2.3.2. Website linked with application not hosted at eGA	13
2.3.3. Website developed by eGA and embedded with application developed by eGA	15
2.3.4. Website developed by eGA and embedded with application developed by Public Institution	15
2.3.5. Website developed by Public Institution and embedded with application developed by eGA	16
2.3.6. Website developed by Public Institution and embedded with application developed by Public Institution.	16
2.4. Dedicated Hosting Services	16
2.4.1. Virtualized Environment	17
2.4.2. Physical Environment	19
2.5. Co-location Services	19
2.5.1. Co-located in Data Centre shared network	20
2.5.2. Co-located in self-managed network	21
3. IMPLEMENTATION, REVIEW AND ENFORCEMENT	22
4. GLOSSARY AND ACRONYMS	22
4.1 Acronyms	22
5. RELATED DOCUMENTS	22
6. DOCUMENT CONTROL	22

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

1. OVERVIEW

1.1 Introduction

The e-Government Agency is established under the Executive Agency Act No.30, 1997, Cap 245 as a semi-autonomous Institution under President's Office Public Service Management and Good Governance. eGA is charged with the mandate of providing coordination, oversight and provision of e-Government initiatives and enforcement of e-Government standards to Public Institutions. In executing its duties, eGA shall implement and maintain a coordinated Government operations for Information and Communication Technology (ICT) that include the formulation of standards, technical guidelines and procedures to effectuate the purpose of the Agency.

Some of Public Institutions that get eGovernment services from eGA, believe that they bear zero responsibility for securing their systems, pointing to the need for a more comprehensive guide that makes ICT security everyone's business. Security responsibilities guidelines are conditions, requirements and procedures that should be adhered to before, during and after provision of or receiving of eGovernment Agency services such as websites, applications and co-location hosting services. It stipulates the roles and responsibilities of Public Institutions that should be performed throughout the period of receiving eGovernment services from eGA and also stipulates the roles and responsibilities of service provider (eGA) to ensure that the service provided is in line with e-Government standards and guidelines.

Cybersecurity risks can never be eliminated completely, but they can be mitigated to reduce the impact of threats and breaches. This document contains the guidelines that clears out security responsibilities in e-Government Agency owned or controlled facilities and points out the roles and responsibilities of each party involved.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

1.2 Rationale

eGovernment services are being provided to Public Institutions without binding the Public Institutions security responsibilities to the Public Institutions themselves. As a result, some Public Institutions neither prepare budget nor get prepared to resolve cybersecurity challenges, believing that everything should be handled by eGA. Cyber security protection cannot be achieved if everyone is not involved in the fight. Therefore, it is critical to state categorically the roles of the Agency and the security prerequisites that must be fulfilled by Public Institutions that receive eGovernment services from eGA.

1.3 Purpose

The general objective of this document is to pinpoint specific ICT security roles and responsibilities for both service recipient (Public Institution) and service provider (eGA) during the entire cycle of eGovernment service provisioning. More specifically, the document:

- a) Enriches understanding and minimize complains to eGA during and after cyber security incidents;
- b) Ensures all Public Institutions understand and accept their ICT security responsibilities before deciding to use eGovernment Agency services; and
- c) Aligns ICT security responsibilities with the eGovernment Agency services contracts.

1.4 Scope

This document is applicable to e-Government services provided by eGA and Public Institutions that are requesting or receiving such services from eGA. The services referred by this document are website services, application services, services for website connected with applications, dedicated hosting services and co-location services.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

2. GUIDELINES FOR SECURITY RESPONSIBILITIES

A Public Institution wishing or required to use eGovernment Services from eGA, especially those services that relate to innovation, designing, creation, development, purchase, support, operating and maintaining information systems must have cybersecurity considerations at uttermost attention. The Public Institutions must therefore do its responsibilities with regards to protecting its information, in course of using eGA services. General Public Institution responsibility is to **comply with eGovernment Standards that require a Public Institution, to report to eGA for advice, when planning to build and host an eGovernment application system.** The Public Institution is required to include ICT security on every stage of system design and development and involve eGA for security consultancy whenever necessary. A system, will not be hosted in Government Data Centers if it has security weaknesses (It is vulnerable), and therefore Public Institutions must ensure that the system has undergone a thorough security check before requesting for GDC hosting services. This exercise must be properly planned as **last minute security checks might result into delays in systems go-live.** If the Public Institution has not done security check and needs GDC hosting services, eGA will do that testing, and ensure that the Public Institutions clears all the vulnerabilities before allowing the system to be hosted. Even after getting hosting services, Public Institutions are required to upgrade, patch and clear security flaws in their systems, from time to time, and keep them from becoming vulnerable again. Vulnerable system from Public Institutions that do not do their security responsibilities, soon get infected, and this way infecting, secured system of innocent Public Institutions that are in the same shared environment. eGA does planned and ad-hoc checking of the health of systems hosted in GDC, as well as continuous monitoring and protection of all systems. Where systems are found to be vulnerable, the Public Institution will receive an advisory to clear the vulnerability, and be required to clear the vulnerabilities to qualify to continue getting the hosting services.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

2.1. Website Services

The Agency provides website hosting services for the websites that have been developed in house and those being developed externally by the Public Institutions. The Public Institution chooses the mode of hosting, whether in shared environment or in dedicated environment depending on the complexity of the website and critically of the services provided. Furthermore, websites being developed by free content management system like Joomla, Wordpress and alike, requires the Public Institutions to commit to perform regular updating and upgrading. The Agency checks whether the website to be hosted is compatible to the hosting environment in terms of Databases and Programming Language used before accepting to host the website. Short training is usually provided to Public Institutions for familiarization with Agency hosting environment and methods of uploading web files as well as overall content management. This section guides Public Institutions on ICT security roles and responsibilities for various categories of website hosting services by stipulating what eGA should do and what the Public Institution should do.

2.1.1. Website developed by eGA and hosted by eGA

2.1.1.1. Public Institution Roles and Responsibilities

- a) Whereas, the website was developed by eGA and the source code has been disclosed to the Public Institution and has been given access to make changes to the source code, the Public Institution shall be the sole owner/controller of all website files, scripts, images, designs, or any other electronic content, either local or linked, necessary for the proper functioning or appearance of the website;
- b) The Public Institution shall be the sole owner of the website user data also referred to as the website content which may include, but not limited to, uploaded files, audio, video, images, linked data, etc;

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- c) The Public Institution that has been given access, on request and at own cost, shall ensure that it is trained on administration of their hosting environment;
- d) The Public Institution shall be responsible for safe-keeping of all credentials necessary to access their hosting environment, database(s), website data, and eGA shall not be held responsible in case of disclosure or poor management of website data/credentials done by the Public Institutions;
- e) The Public Institution shall be responsible to report any suspicious issues such as changed or unknown contents on their website to eGA;
- f) ICT Security 'services not in this document' that are provided by eGA, such as website vulnerability assessments, shall be standard services provides by eGA to all Public Institutions as per eGA procedures. Public Institutions requiring special treatment shall stipulate this in the contract/agreements;
- g) Public Institution shall work on any security advisory provided by the eGA and provide implementation feedback to eGA on the same;
- h) Website backups shall be taken by the Public Institution and stored offline to complement the backup done by eGA at interval stipulated in eGA procedures. If specific interval is required, the Public Institution should state the need before hosting of the website in the contract/agreements;
- i) Should there be a need for retrieving old website source code or content, the Public Institution shall place a request to eGA and will be notified of when and what to be obtained and the procedures to be followed;
- j) The hosting environment is shared. Therefore, the Public Institution shall only have control and command of their portion of the hosting environment but are not allowed to perform any action which may

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

affect system-wide parameters and affect other users of shared environment;

- k) If a dedicated hosting environment is required where the Public Institution desires to have full control of the website including system-wide parameters and environmental variables, a different hosting arrangement has to be requested. This means that the Public Institution shall be able and responsible for full administration of their website and hosting environment including, but not limited to, security operations such as system update and patching;
- l) The Public Institution shall provide communication details for Institutional officers responsible for managing the website in the agreement and
- m) Upon advisory either from eGA or website main stream providers and notifications, Public Institutions, that have control of their websites, shall perform regular updates and upgrades.

2.1.1.2. eGA Roles and Responsibilities

- a) eGA shall check security status of websites hosted at an interval specified in Agency procedures;
- b) eGA shall provide Institutions under this category with Security advisories to remediate security discovered from time to time;
- c) The Agency shall provide environment that is as secure as a shared environment can be and suitable for all needs of the Public Institution at the infrastructure level;
- d) In case the website has been compromised, the website shall be put offline from the public access until the incident has been rectified;
- e) eGA shall do backup of the Public Institution website's source code and content on rotation basis as per Agency procedures;

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- f) eGA shall not be responsible for unavailability of backup data or files that are required by the Public Institution but are not available because they are not in Agency standards backup operations intervals and were not stated as a requirement in the contract/agreements;
- g) eGA shall be responsible for providing updates and upgrades for the website it has developed; and
- h) eGA shall ensure there is a proper system for recording and archiving details of each website versions it has developed and update the records whenever changes are made (versioning).

2.1.2. Website developed by Public Institution and hosted at eGA

2.1.2.1. Public Institution Roles and Responsibilities

- a) The Public Institution shall be provided with conditions and options for hosting non-eGA developed websites including the suitable versions and platforms which are accepted, the Public Institution shall choose the best that fits their plans;
- b) If the need arise that necessitate change of hosting environment, the Public Institution shall upgrade their website to meet the new technical requirements within three months of notice period as after that period the environment will be upgraded without further notice;
- c) The Public Institution shall be the sole owner of all website files, scripts, images, designs, or any other electronic content, either local or linked, necessary for the proper functioning or appearance of the website collectively referred to as the source code;
- d) eGA shall not be responsible and accountable in case the Public Institution's website content or source code violates any third-party agreements, rules, regulations, or any other legal or security requirement(s);

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- e) The Public Institution, on request and at own cost, will be trained on administration of their hosting environment;
- f) Due to security reasons, websites developed using free content management systems (CMS) are highly discouraged in eGA shared environment. The Public Institution with free CMS shall be held accountable and removed from shared hosting environment without prior notice if they do not secure their websites. Securing websites developed by using free CMS include doing the following activities;
 - i. If eGA has to host a website developed using free CMS, then the Public Institution must first demonstrate the capability to manage the upgrading/updating process and using up to date extensions;
 - ii. Public Institution's Website administrators must use strong passwords and change them frequently;
 - iii. Public Institution's Website administrators must remove CMS installation folder in the live environment;
 - iv. Public Institution's Website administrators must use security extensions from trusted sources;
 - v. Public Institution's Website administrators must protect the CMS administration URL such as renaming default CMS administration path to a custom path;
 - vi. Public Institution's Website administrators must update the CMS and extension every month and must send the update evidence to eGA every two months via updates@ega.go.tz; and
 - vii. Public Institution's must acknowledge in writing that the website will be put in halt if no updates evidence are received for five months consequently.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- g) The Public Institution shall ensure that a website comply with the Agency hosting requirements and abide with the guidelines in this document;
- h) The Public Institution shall bear website security responsibilities for the website that is not developed by eGA. If the Public Institution wishes to delegate part of its security responsibilities to eGA, the delegation must be clearly stated in the contract/agreements; and
- i) The Public Institution shall also have the responsibilities in 2.1.1.1 (d), (f), (j) and (k) for this category as well.

2.1.2.2. eGA Roles and Responsibilities

- a) The Agency shall be responsible to provide the specification for hosting environment and available options for performance and security of the website, the Public Institution is responsible for their choice;
- b) The Agency shall review security reports for the website to be hosted (if any) or arrange security check prior to acceptance for hosting at eGA facility; and
- c) The Agency shall also have the responsibilities in 2.1.1.2 (a) to 2.1.1.2 (h) for this category as well.

2.1.3. Website developed by eGA and not hosted at eGA

2.1.3.1. Public Institution Roles and Responsibilities

- a) The Public Institution shall be the sole owner/controller of all website files, scripts, images, designs, or any other electronic content, either local or linked, necessary for the proper functioning or appearance of the website; and
- b) The Public Institution shall be responsible for all website security and operational related matters including but not limited to

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

upgrading, updating, availability, integrity and confidentiality of the website.

2.1.3.2. eGA Roles and Responsibilities

- a) Since eGA has no any control over the website, all the website security and non-security roles will be solely responsibility of the Public Institution; and
- b) The Agency shall also have the responsibilities in 2.1.1.2 (g) in this category as well.

2.2. Application Services

The Agency develops and host different types of applications for Public Institutions to improve service delivery. Both web-based and locally deployed application are being developed and hosted. Public Institutions may demand to host the application at their own facility or leave it to the Agency regardless of whether the Agency developed it. In either case both Public Institutions and the Agency will have roles to play to ensure best performance of the application. This section guides Public Institutions on ICT security roles and responsibilities for various categories of application services by stipulating what eGA should do and what the Public Institution should do.

2.2.1. Application developed by eGA and hosted by eGA

2.2.1.1. Public Institution Roles and Responsibilities

- a) The Public Institution shall also have the responsibilities in 2.1.1.1 (a) to (m) with regards to applications developed by eGA and hosted by eGA.

2.2.1.2. eGA Roles and Responsibilities

- a) The Agency shall also have the responsibilities in 2.1.1.2 (a) to (h) with regards to applications developed by eGA and hosted by eGA.

**THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY**

2.2.2. Application developed by Public Institution and hosted by eGA

2.2.2.1. Public Institution Roles and Responsibilities

- a) The Public Institution shall also have the responsibilities in 2.1.2.1 (a) to (k) with regards to applications developed by themselves and hosted by eGA.

2.2.2.2. eGA Roles and Responsibilities

- a) The Agency shall also have the responsibilities in 2.1.2.2 (a) to (c) with regards applications developed by Public Institution and hosted by eGA.

2.2.3. Application developed by eGA and not hosted at eGA

2.2.3.1. Public Institution Roles and Responsibilities

- b) The Public Institution shall also have the responsibilities in 2.1.3.1 (a) to (c) with regards to applications developed by eGA and hosted somewhere else.

2.2.3.2. eGA Roles and Responsibilities

- a) The Agency shall also have the responsibilities in 2.1.3.2 (a) with regards to applications developed by eGA and hosted somewhere else.

2.3. Website connected with Application

Websites that are being hosted by the Agency are sometimes linked/embedded with applications. Linked to application means that the website communicates/links with the application that is hosted independently with the website or outside Agency hosting facility. In this case, the website and application are in separate environments. Embedded with application means both the website and application are hosted on the same environment, inside one folder for example. In either scenario, the Agency and the Public Institution have different roles and responsibilities to perform for proper functioning of the website. This

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

section guides Public Institutions on ICT security roles and responsibilities for various categories of services where websites are connected with application by stipulating what eGA should do and what the Public Institution should do.

2.3.1. Website linked with Application hosted at eGA

2.3.1.1. Public Institution Roles and Responsibilities

- a) Where the website or application is developed by the Agency, then the Public Institution shall also have the responsibilities in 2.1.1.1 (a) to 2.1.1.1. (m) in relation to this website or application; and
- b) Where the website or application is developed by the Public Institution, then the Public Institution shall also have the responsibilities in 2.1.2.1 (a) to 2.1.2.1 (k) in relation to this website or application

2.3.1.2. eGA Roles and Responsibilities

- a) Where the website or application is developed by the Agency then the Agency shall also have the responsibilities in 2.1.1.2 (a) to 2.1.1.2 (h) in relation to website or application; and
- b) Where the website or application is developed by the Public Institution, then the Agency shall also have the responsibilities in 2.1.2.2 (a) to 2.1.2.2 (c) in relation to website or application.

2.3.2. Website linked with application not hosted at eGA

2.3.2.1. Public Institution Roles and Responsibilities

- a) If the website was developed by the Agency then the Public Institution also has the responsibilities in 2.1.1.1 (a) to 2.1.1.1. (m) for this category as well;

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- b) If the website was developed by the Public Institution, then the Public Institution also has the responsibilities in 2.1.2.1 (a) to 2.1.2.1 (k) for this category as well;
- c) If the application was developed by eGA and not hosted at eGA, then Public Institution has the responsibilities in (a) to (c) with regards to the application; and
- d) If the website is communicating with the Application using API or other means provided by the Public Institution then:
 - i. Public Institution shall ensure that there is a secure communication between the site and the provided API;
 - ii. Public Institution shall ensure confidentiality of the shared communication credentials that are used by the site;
 - iii. Public Institution shall be responsible for the security and availability of the application;
 - iv. The Public Institution shall be responsible for providing and securing credentials that has been shared with the third party; and
 - v. Any additional service that may be required from eGA the Public Institution should stipulate clearly before the hosting service is provided.

2.3.2.2. eGA Roles and Responsibilities

- a) If the website was developed by the Agency then the Agency also have the responsibilities in 2.1.1.2 (a) to 2.1.1.2 (h) for this category as well;
- b) If the website was developed by the Public Institution, then the Agency also have the responsibilities in 2.1.2.2 (a) to 2.1.2.2 (c) for this category as well; and
- c) If the application was developed by eGA and not hosted at eGA, then the Agency also have the responsibilities in 2.1.3.2 for this category as well.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

2.3.3. Website developed by eGA and embedded with application developed by eGA

2.3.3.1. Public Institution Responsibilities

- a) Public Institution should be aware that website files and application files are in the same place, therefore Public Institution shall ensure any modification done in the application do not affect the website; and
- b) The Public Institution also have the responsibilities in 2.1.1.1 (a) to 2.1.1.1 (m) for this category as well, except 2.1.1.1 (k).

2.3.3.2. eGA Roles and Responsibilities

- a) The Agency shall also have the responsibilities in 2.1.1.2 (a) to 2.1.1.2 (h) for this category as well.

2.3.4. Website developed by eGA and embedded with application developed by Public Institution

2.3.4.1. Public Institution Roles and Responsibilities

- a) The Public Institution shall also have the responsibilities 2.3.3.1 (a) in for this category as well;
- b) The Public Institution shall also have the responsibilities in 2.1.1.1 (a) to 2.1.1.1 (m) for this category as well except 2.1.1.1 (k); and
- c) The Public Institution shall also have the responsibilities in 2.1.2.1 (a) to (k) with regards to this application.

2.3.4.2. eGA Roles and Responsibilities

- a) The Agency shall also have the responsibilities in 2.1.1.2 (a) to 2.1.1.2 (h) for this category as well; and
- b) The Agency shall also have the responsibilities in 2.1.2.2 (a) to (c) with regards to this application.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

2.3.5. Website developed by Public Institution and embedded with application developed by eGA

2.3.5.1. Public Institution Roles and Responsibilities

- a) The Public Institution shall also have the responsibilities in 2.1.2.1 (a) to 2.1.2.1 (k) for this category as well;
- b) The Public Institution shall also have the responsibilities in 2.1.1.1 (a) to (m) with exception of 2.1.1.1(k) with regards to this application.

2.3.5.2. eGA Roles and Responsibilities

- a) The Agency shall also have the responsibilities in 2.1.2.2 (a) to 2.1.2.2 (c) for this category as well; and
- b) The Agency shall also have the responsibilities in 2.1.1.2 (a) to (h) with regards to this application.

2.3.6. Website developed by Public Institution and embedded with application developed by Public Institution.

2.3.6.1. Public Institution Roles and Responsibilities

- a) Since website or application was developed by the Public Institution, then the Public Institution shall also have the responsibilities in 2.1.2.1 (a) to 2.1.2.1 (k) in relation to website/application.

2.3.6.2. eGA Roles and Responsibilities

- a) Since the website or application was developed by the Public Institution, then the Agency shall also have the responsibilities in 2.1.2.2 (a) to 2.1.2.2 (c) in relation to website/application.

2.4. Dedicated Hosting Services

Upon reaching the decision to host application at eGA, the Public Institution is required to provide detailed requirements in terms of storage, bandwidth, operating system, database, number of concurrent users and other related requirements. Prior to provisioning of the service, eGA advises the Public Institution to opt for either dedicated or shared environment as it is the Public

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

Institution that understands the criticality of the application. This is because ***dedicated environments are more secure than shared environments but are also more expensive.*** And so it is important that the Public Institution establish how critical is the application before deciding to host it in shared or dedicated environment. Once the virtualized or physical dedicated environment is provided to the Public Institution, the responsibilities for installation, configuration and other setup activities are left to be done by the Public Institutions themselves; however the Agency may offer technical support whenever requested to do so. The Agency cannot access the Public Institution application rather has to ensure the hosting environment is up and running. This section guides Public Institutions on ICT security roles and responsibilities for various categories of dedicated hosting services by stipulating what eGA should do and what the Public Institution should do.

2.4.1.Virtualized Environment

2.4.1.1. Public Institution Roles and Responsibilities

- a) Monitoring: Public Institution is responsible for monitoring resources which are allocated to application including storage, processor, and memory utilization;
- b) Backup/restore services: Public Institution is required to make regular (daily/weekly) offsite backups of a database(s) and application files;
- c) Updates and upgrades: A Public Institution is responsible to make sure that it is using the latest and stable operating system;
- d) Credentials disclosure: Public Institution shall be responsible for keeping credentials securely;
- e) Operation Tasks: All daily operation tasks are Public Institution responsibilities, upon request, Agency may offer technical support;

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- f) Licensing: A Public Institution is responsible for management of software licensing of application with exception for software licenses provided by eGA;
- g) Security issues: A Public Institution is responsible to make sure applications, databases and operating systems are properly secured including managing patches and updates; and
- h) Other roles with regards to application, the Public Institution also have the responsibilities as in section 2.2.

2.4.1.2. eGA Roles and Responsibilities

- a) Monitoring: eGA is responsible for basic monitoring of hosting resources including servers, storage, and network;
- b) Environments to be hosted: eGA will provide highly available environment for application hosting;
- c) Backup/restore services and disaster recovery: In case of disaster involving hosting resources, eGA will provide environment which will facilitate minimal downtime using offsite backup made by a Public Institution;
- d) Access: eGA will provide all privileged access to application hosting environment;
- e) Licensing: eGA is responsible for management of software licensing of application on for licenses provided by eGA; and
- f) Maintenance: eGA is responsible to ensure that the infrastructure hosting the applications is in good condition for optimal performance and provide specification when the application is to be hosted by the Public Institution

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

2.4.2. Physical Environment

2.4.2.1. Public Institution Roles and Responsibilities

- a) The Public Institutions also have the responsibilities in 2.4.1.1 (a) to (h) for this category as well.

2.4.2.2. eGA Roles and Responsibilities

- a) Hardware Support: eGA will be responsible for the maintenance/repair/replacement of the hardware rented and ensure its sustainable performance; and
- b) The Agency should also have the responsibilities in for 2.4.1.2 (a) to 2.4.1.2 (f) this category as well.

2.5. Co-location Services

The Agency offers an environment whereby Government institutions rents space within the Government Datacenters (GDC) owned or managed by eGA for the purpose of providing conducive, secure and reliable environment for hosting equipment (servers, storages, networking equipment). The service is offered from small (U) space, to half and full rack space depending on the Public Institution's requirements. This is common when the Public Institutions wishes to have better environment to host their equipment that is conducive, reliable and secure. The Agency therefore, provides a rental space with reliable power supply systems, cooling systems and physical security systems. The Public Institutions brings in equipment that occupies a unit, part of rack or the whole rack to the rented space. Prior to acceptance of Public Institution equipment, detailed requirements are submitted to the Agency. After the Agency confirms that it can meet the Public Institution requirements, the equipment are moved to the Data Centre. This section guides Public Institutions on ICT security roles and responsibilities for various categories of co-location services by stipulating what eGA should do and what the Public Institution should do.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- f) Licensing: A Public Institution is responsible for management of software licensing of application with exception for software licenses provided by eGA;
- g) Security issues: A Public Institution is responsible to make sure applications, databases and operating systems are properly secured including managing patches and updates; and
- h) Other roles with regards to application, the Public Institution also have the responsibilities as in section 2.2.

2.4.1.2. eGA Roles and Responsibilities

- a) Monitoring: eGA is responsible for basic monitoring of hosting resources including servers, storage, and network;
- b) Environments to be hosted: eGA will provide highly available environment for application hosting;
- c) Backup/restore services and disaster recovery: In case of disaster involving hosting resources, eGA will provide environment which will facilitate minimal downtime using offsite backup made by a Public Institution;
- d) Access: eGA will provide all privileged access to application hosting environment;
- e) Licensing: eGA is responsible for management of software licensing of application on for licenses provided by eGA; and
- f) Maintenance: eGA is responsible to ensure that the infrastructure hosting the applications is in good condition for optimal performance and provide specification when the application is to be hosted by the Public Institution

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

2.4.2. Physical Environment

2.4.2.1. Public Institution Roles and Responsibilities

- a) The Public Institutions also have the responsibilities in 2.4.1.1 (a) to (h) for this category as well.

2.4.2.2. eGA Roles and Responsibilities

- a) Hardware Support: eGA will be responsible for the maintenance/repair/replacement of the hardware rented and ensure its sustainable performance; and
- b) The Agency should also have the responsibilities in for 2.4.1.2 (a) to 2.4.1.2 (f) this category as well.

2.5. Co-location Services

The Agency offers an environment whereby Government institutions rents space within the Government Datacenters (GDC) owned or managed by eGA for the purpose of providing conducive, secure and reliable environment for hosting equipment (servers, storages, networking equipment). The service is offered from small (U) space, to half and full rack space depending on the Public Institution's requirements. This is common when the Public Institutions wishes to have better environment to host their equipment that is conducive, reliable and secure. The Agency therefore, provides a rental space with reliable power supply systems, cooling systems and physical security systems. The Public Institutions brings in equipment that occupies a unit, part of rack or the whole rack to the rented space. Prior to acceptance of Public Institution equipment, detailed requirements are submitted to the Agency. After the Agency confirms that it can meet the Public Institution requirements, the equipment are moved to the Data Centre. This section guides Public Institutions on ICT security roles and responsibilities for various categories of co-location services by stipulating what eGA should do and what the Public Institution should do.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

2.5.1.Co-located in Data Centre shared network

2.5.1.1. Public Institution Roles and Responsibilities

- a) The Government entity shall be solely responsible for maintaining the security of the systems and the associated software installed within the co-located equipment. This shall include upgrading and patching of operating systems, Database Management Systems and other related software;
- b) The Public Institution shall be required to adhere with the data center standards and guidelines;
- c) Remote access to co-located network equipment shall be provided through de-facto authentication on Secure Shell (SSH) over a P2P L2 IPsec VPN between Government entity HQ and GDC; and
- d) The Public Institution shall need to ensure the equipment which will be moved in to the datacenter have an operational disaster recovery site (DR site) and hence very minimal service disruption shall be caused as a result of moving equipment into the datacenter.

2.5.1.2. eGA Roles and Responsibilities

- a) Hardware Support: eGA shall be required to provide access to the datacenter in accordance with the GDC guidelines and procedures for any issue that may require Public Institutions' access to the data center. The Agency shall also be responsible for the maintenance/repair/replacement of the Agency network devices to ensure they are up and running;
- b) Security: eGA will be responsible for physical and network security of co-located hardware(s) which are solely connected to GDC network;
- c) The Agency should assist with VPN connection as in 2.5.1.1 (c) with regards to Agency roles;

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

- d) Physical access to the server: This is guided by Government Datacenter procedures that shall be disclosed to the Public Institution before service provision;
- e) eGA shall be responsible to ensure the physical security of the co-located equipment is maintained by allowing the required logical services as requested by the Government entity; and
- f) The Agency should also ensure there is systems redundancy in line with eGovernment standards as per 2.5.1.1 (d).

2.5.2.Co-located in self-managed network

2.5.2.1. Public Institution Roles and Responsibilities

- a) The Public Institution shall also have the responsibilities in 2.5.1.1 (a) to 2.5.1.1 (d) for this category as well;
- b) If the Public Institution has been collocated with her own independent Internet Service Provider, the Public Institution shall be liable for her own network security with her service provider;
- c) If the Public Institution has been co-located and uses her own network devices, the Public Institution shall be liable for configuration and maintenance of those network devices; and
- d) If network devices belong to the Agency, then the Public Institution shall be responsible for the configuration and security of the virtual network provided.

2.5.2.2. eGA Roles and Responsibilities

- a) The Agency shall also have the responsibilities in 2.5.1.2 (a) to 2.5.1.2 (f) for this category as well.

THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT
e-GOVERNMENT AGENCY

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

- 3.1 This document shall be effective upon being signed on its first page.
- 3.2 This document shall be subjected to review at least once every year or whenever necessary changes are needed

4. GLOSSARY AND ACRONYMS

4.1 Acronyms

CMS	Content Management System
eGA	e-Government Agency
GDC	Government Data Centre
ICT	Information and Communication Technology
LGA	Local Government Authority
MDA	Ministry, Department, Agency
VPN	Virtual Private Network

5. RELATED DOCUMENTS

- 5.1. Government Data Centre Guideline and Procedures
(eGA/EXT/IRA/002)
- 5.2. eGovernment Security Architecture – Standards and Technical
Guidelines (eGA/EXT/ISA/001)

6. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	eGA	Creation of document	July 2019