




THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE, PUBLIC SERVICE MANAGEMENT AND GOOD
GOVERNANCE
e-GOVERNMENT AUTHORITY

Document Title

e-Government Security Operations Guidelines

Document Number

eGA/EXT/ISA/004

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Mussa M. Kissaka	Board Chairperson		25/08/2023

PREFACE

In the last few decades, the use of ICT as enabler for improving Government operations and service delivery to citizens has not only become significant but also inevitable pre-requisite for enhancing operational efficiency and effectiveness. In the quest of reaping the benefits brought about by the use of ICT, it was apparent for enactment of the e-Government Act No. 10 of 2019 and its Regulations that was declared through the Government Notice No. 75 of February 7, 2020, which provided guidance on proper approach for implementing e-Government. The Act also established e-Government Authority with the mandate of coordinating, promoting and overseeing e-Government implementation as well as enforcing compliance with laws, regulations, standards and guidelines related to e-Government implementation in Public Institutions.

To ensure confidentiality, availability and integrity of Government ICT services to citizens, Sections 37 through 46 of the e-Government Act requires public institutions to perform various ICT operations to strengthen public institutions ICT security posture. The Authority, through the e-Government Security Operations Center (e-GSOC) has been mandated to enforce rules, strategies, standards, guidelines and procedures for implementation of e-Government security. Pursuant to these provisions, the Authority through the e-Government Security Operations Center (e-GSOC) has prepared this document to prescribe guidelines for performing and reporting various ICT security operations in public institutions.



Dr. Mussa M. Kissaka

BOARD CHAIRPERSON

Table of Contents

1. INTRODUCTION	3
1.1 Overview	3
1.2 Purpose	3
1.3 Rationale	4
1.4 Scope	4
2. THE GUIDELINES.....	5
2.1 Guidelines for Government ICT Security Single Point of Contact (SPOC).....	5
2.2 Guidelines for ICT Security Governance and Management	5
2.3 Guidelines for General ICT security Operations	6
2.4 Guidelines for User Access Management	7
2.5 Guidelines for ICT Security Risk Assessment.....	8
2.6 Guidelines for ICT Security Assessment and Audit.....	8
2.7 Guidelines for Incident Management and Disaster Recovery	10
2.8 Guidelines for ICT Security Human Resource	11
2.9 Guidelines for Security of endpoint ICT Equipment	11
3. IMPLEMENTATION, REVIEW AND ENFORCEMENT	11
4. GLOSSARY AND ACRONYMS	12
4.1 Glossary.....	12
4.2 Acronyms	12
5. RELATED DOCUMENTS.....	13
6. DOCUMENT CONTROL	13
Appendix I: For the purposes of this guideline, Vulnerabilities Risk Rating Criteria depends on Common Vulnerability Scoring System (CVSS) which depends on exploitability, propagation and impact.....	14
Appendix II: ICT Security Assessment Compliance Criteria	15

1. INTRODUCTION

1.1 Overview

The e-Government Authority also known as "e-GA" is a public institution established under the e-Government Act, 2019 mandated to coordinate, oversee and promote e-Government initiatives and enforce e-Government related policies, laws, regulations, standards and guidelines in Public Institutions. Regulation 45 of e-Government General regulations 2020 requires the Authority through e-Government Security Operations Center to develop mechanism for enforcement of rules, strategies, standards, guidelines and procedures for implementation of e-Government security as provided in the Act.

Pursuant to the provisions of section 37 to section 46 of the e-Government Act, 2019, public institutions shall for the purpose of ICT security, perform various operations to enhance their ICT security posture. Further, pursuant to the provision of section 36(1) of the e-Government Act, the Government has established the e-Government Security Operations Center (e-GSOC) to enforce rules, strategies, standards, guidelines and procedures for implementation of e-Government security in public institutions. To ensure effective and efficient coordination and management of ICT security in public institutions, e-GSOC has prepared guidelines for ICT security operations in public institutions to provide detailed information on how public institutions may enhance protection of ICT systems and infrastructure against security threats while maintaining compliance with the security and legal requirements for confidentiality, privacy, accessibility, availability and integrity, as referred in *e-Government Security Architecture – Standards & Technical Guidelines (eGA/EXT/ISA/001)*.

1.2 Purpose

The purpose of this document is to provide specific guidelines to public institutions on how to conduct and report various ICT security initiatives and operations.

1.3 Rationale

As the number of ICT security breaches and the cost of data loss in ICT systems is increasing year over year, organizations and Governments are being forced to shift their focus from not only leveraging ICT solutions, but also to preventing, detecting and responding to various cyber security threats. For the purpose of effective and efficient ICT security governance and management, this document provides guidelines to conduct and report various ICT security initiatives and operations in public institutions.

1.4 Scope

This document shall be used by all public Institutions during operationalization of various ICT security strategies and operations.

2. THE GUIDELINES

2.1 Guidelines for Government ICT Security Single Point of Contact (SPOC)

To ensure effective handling of various ICT security matters in the Government:

2.1.1 Public institution shall appoint one (1) ICT officer among its ICT Staff to be an institutional ICT Security Single Point of Contact (SPOC).

2.1.2 Duties of the institutional ICT Security Single Point of Contact shall be among others be:

- a) To advice and coordinate initiatives regarding compliance to e-Government Act, Regulation, standards and Guidelines in areas related to ICT security matters.
- b) To communicate various institutional cyber security initiatives to e-Government Security Operations Center (e-GSOC) and
- c) To participate and respond to institutional cyber security incidents.

2.1.3 The SPOC appointment letter shall be sent to e-GA and shall include the appointed SPOC full names, phone number and official email address.

2.1.4 Public institution shall immediately inform e-Government Authority (e-GA) when there is change in the appointed institutional ICT Security Single Point of Contact (SPOC).

2.1.5 Public institution shall create an ICT security e-mail with the format of "ictsecurity@domain" e.g. ictsecurity@ega.go.tz for communication on ICT security matters between public institution and e-Government Security Operations Center (e-GSOC).

2.1.6 Institutional ICT security e-mail shall be configured to ensure that all e-mails delivered to it are also forwarded to at least Accounting Officer, Head of ICT Unit and ICT security Single Point of Contact (SPOC) e-mail addresses.

2.2 Guidelines for ICT Security Governance and Management

For the purpose of implementation of Government Cyber Security Strategy (GCSS), public institution shall:

- 2.2.1 Ensure that institutional ICT security policy and ICT security strategy are aligned with Government Cyber Security Strategy (GCSS).
- 2.2.2 Submit through Government ICT Services Portal (GISP) approved institutional ICT Security Policy and ICT Security Strategy.
- 2.2.3 Prepare and submit through Government ICT Services Portal (GISP), the report on the implementation of Government Cyber Security Strategy (GCSS) within fourteen (14) days after the end of each financial year.

2.3 Guidelines for General ICT security Operations

A public institution shall ensure:

- 2.3.1 ICT security requirements that comply with institutional ICT security policy and strategy are included and implemented during development and acquisition of institutional ICT systems.
- 2.3.2 After deployment of an ICT system, all business operations are performed by business process owners and not vendors/developers.
- 2.3.3 Systems and Applications operate with valid licenses, stable and supported software versions with appropriate patches and updates.
- 2.3.4 Performing of ICT security assessment before deploying application(s) to production environment or when significant change(s) has been made to the application.
- 2.3.5 Having correct statistics of ICT systems and devices through proper ICT assets management and ensure that systems that are not used or are for testing are removed from the network (or from public access and/or production environment).
- 2.3.6 Monitoring of ICT systems and infrastructure is done by:
 - a) Continuously perform monitoring all ICT Systems and Networks using available technologies and tools;
 - b) Analyzing logs for unusual activity that could indicate attacks to institutional systems.
- 2.3.7 Management and control of removable media is done by:

- a) Incorporating in the institutional ICT policy/ICT security policy, procedures to controls access and usage of removable media; and
- b) Scanning all media for malware before importing onto corporate systems.

2.4 Guidelines for User Access Management

A public institution shall ensure adequate management of user access and privileges by:

- a) Authenticating and authorizing all application(s) and network users based on their verified business needs before granting access;
- b) Restricting usage of generic accounts such as “admin”, “auditor”, etc. during authentication into ICT systems, instead all users must be authenticated and logged in with their own specific accounts;
- c) Restricting usage of shared accounts to access ICT systems;
- d) Establishing the process for registration and de-registration of user accounts to ensure that all accounts that do no longer require access/privileges to systems are forbidden/disabled from accessing ICT systems resources;
- e) Limiting the number of high privileged accounts and limiting user privileges according to their activities;
- f) Monitoring user activities, control access to users’ activities and audit logs; and
- g) Regularly audit the usage of high privileged accounts in ICT systems.

2.5 Guidelines for ICT Security Risk Assessment

- 2.5.1 For the purpose of ICT security risk management, public institution shall conduct ICT security risk assessment at least once annually.
- 2.5.2 ICT security risk assessment shall be conducted by using respective public institution internal human resource or by seeking guidance from e-Government Authority (e-GA).

2.6 Guidelines for ICT Security Assessment and Audit

A public institution shall ensure that:

- 2.6.1 It conducts ICT Security vulnerability assessments and penetration tests at least semiannually depending on the results of risk assessment.
- 2.6.2 Institution ICT security assessments and audits cover essential institution ICT systems such as Networks Infrastructure, Operating Systems, application software, workstations and servers, database applications as well as institutional ICT security management.
- 2.6.3 ICT security vulnerability assessments and penetration tests are conducted by using respective public institution internal human resource or by seeking guidance from e-Government Authority (e-GA).
- 2.6.4 Assessment of application and software include but not limited to assessing application's identity management, user authentication and access management, segregation of duties, session management, input validation, error handling, security misconfiguration, testing of weak cryptography and application audit trails.
- 2.6.5 Web based applications shall be tested against the latest Open Web Application Security Project (OWASP) Top 10 vulnerabilities methodology, among other methodologies.
- 2.6.6 Mobile applications shall be tested against the latest OWASP Mobile Top 10 vulnerabilities methodology, among other methodologies.
- 2.6.7 Assessment of network infrastructure include among others, assessment on network segmentation and network access controls, secure hardening of

configuration of network devices such as switches, routers, firewall and wireless access points, identification and monitoring of network remote access such as Virtual Private Network (VPN) and Remote Desktop Protocol (RDP).

- 2.6.8 Assessment of servers and workstations include among others, assessment of operating system and applications patch and upgrade management, the use of supported and up-to-date operating system, OS security update configuration, operating system remote access configuration and management, file share access controls and management, presence of centralized end-point protection solution.
- 2.6.9 Vulnerability assessment and penetration test grading/scoring criteria is based on Common Vulnerability Scoring System (CVSS) as depicted in Appendix I and II. Based on Appendix II, if a Public Institution gets *Adequate, Good or Very Good* Score (a score of greater than 40%), then institutional ICT security posture and compliance score is ACCEPTABLE and if a Public Institution gets *Inadequate or Very Inadequate* Score (A score of 40% or less), then institutional ICT security posture and compliance score is UNACCEPTABLE; and
- 2.6.10 Upon completion of an ICT security vulnerability assessment and penetration testing, public institutions submit the report to e-GA through Government ICT Services Portal (GISP).

2.7 Guidelines for Incident Management and Disaster Recovery

Public institution shall ensure:

- 2.7.1 Presence of disaster recovery plan (DRP) and it shall be tested at least semiannually.
- 2.7.2 Disaster recovery tests include all components of disaster recovery plan such as people, process and associated technologies such infrastructures, applications and servers.
- 2.7.3 Disaster recovery plan test reports are prepared and submitted to e-GA through GISP.
- 2.7.4 Taking offline backup (data, application and configuration) periodically as per results of the performed risk assessment. Backups shall never be stored within the same production server.
- 2.7.5 Upon occurrence of significant cyber security incidents, public institution immediately reports the incident to e-GA via e-Government Security Operation Center – eGSOC (egsoc@ega.go.tz) for notification and necessary assistance if required.
- 2.7.6 An incident will be considered significant if:
 - a) It has halted any of the core organization business processes;
 - b) It has affected system(s) that provides services to more than one public institution;
 - c) It has resulted into damage or loss of any key data or information for proper functioning of the institution;
 - d) It has affected multiple ICT systems in a public institution; and
 - e) It has damaged the reputation of public institution or Government.
- 2.7.7 After handling a significant cyber security incident, an institution shall register the incident in GISP for records and reporting purposes.

2.8 Guidelines for ICT Security Human Resource

For the purpose of human resource security, public institution shall:

- 2.8.1 Provide ICT security awareness to all staff at least semiannually.
- 2.8.2 Ensure that security awareness among other things include acceptable use of ICT resources, emerging cyber threats targeting users, e.g. phishing and password management.
- 2.8.3 Provide at least one (1) ICT security technical training annually to ICT staff(s) responsible for ICT security matters.
- 2.8.4 Submit annual ICT security awareness and technical training reports to the Authority through GISP.

2.9 Guidelines for Security of endpoint ICT Equipment

For the purpose of enhancing security of endpoint ICT equipment, public institution shall:

- 2.9.1 Ensure that all institutional endpoint ICT equipment are included in the institutional ICT asset register. For the purpose of this section, endpoint ICT equipment means the ICT equipment that allows entry to a network system.
- 2.9.2 Include and operationalize means, procedures and tools to protect endpoint ICT equipment such as:
 - a) Establishment of a documented plan for endpoint equipment hardening, patching and upgrade management; and
 - b) Deployment and management of a centralized endpoint security protection solutions such as Anti-Virus and anti-malware tools.
- 2.9.3 Inform all users of ICT endpoint equipment particularly computers and mobile devices on their obligations and responsibilities for ICT security, through “Acceptable ICT Use Policy, etc.” during usage of ICT services and equipment.

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

This document shall be:

- 3.1 Effective upon being reviewed and approved by the board and signed by the Board Chairperson.
- 3.2 Subjected to review at least once every three years or whenever necessary changes are needed.
- 3.3 Consistently complied with, any exceptions to its application must duly be authorized by the Board.

4. GLOSSARY AND ACRONYMS

4.1 Glossary

Term	Definitions
e-Government Security	Protecting Government ICT systems and infrastructure against ICT security threats
Vulnerability assessment	The process of examining the ability of an ICT system to withstand cyber attacks
Penetration testing	Authorized simulation attack to an ICT system to evaluate its security strength

4.2 Acronyms

Abbreviation	Explanation
CVSS	The Common Vulnerability Scoring System
e-GA	e-Government Authority
e-GSOC	e-Government Security Operations Center
GCSS	Government Cyber Security Strategy
GISP	Government ICT Services Portal
ICT	Information and Communication Technology
OWASP	The Open Worldwide Application Security Project
RDP	Remote Desktop Protocol
SPOC	Single Point of Contact for ICT security matters
VPN	Virtual Private Network

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. Government Hardware and Software Specification (eGA/EXT/IRA/005).
- 5.4. e-Government Act, 2019.
- 5.5. e-Government General Regulations, 2020.
- 5.6. Guidelines for Development, Acquisition, Operation and Maintenance of e-Government Applications (eGA/EXT/APA/006)
- 5.7. Mwongozo wa Matumizi Bora, Sahihi, na Salama ya Vifaa na Mifumo Ya Teknolojia ya Habari na Mawasiliano (TEHAMA) Serikalini 2022.

6. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	e-GA	Creation of Document	July, 2023

Appendix I: For the purposes of this guideline, Vulnerabilities Risk Rating Criteria depends on Common Vulnerability Scoring System (CVSS) which depends on exploitability, propagation and impact.

S/N.	RISK	CVSS	DEFINITION
1.	None	0.0	A vulnerability is informational with no risks to the institution.
2.	Low	0.1 - 3.9	A vulnerability that is extremely difficult to exploit, or its impact is minimal. Systems with this risk level may be fixed from time to time as may seem possible.
3.	Medium	4.0 - 6.9	A vulnerability is not extremely difficult to exploit given the significance of the data under the systems. Systems involving this risk level should be evaluated and their source of vulnerabilities be fixed as soon as possible
4.	High	7.0 - 8.9	A vulnerability whose exploits might be publicly available and that high confidentiality, integrity and availability impacts may bring loss to the institution. Fixing the issues should be a priority and be done as immediate as possible
5.	Critical	9.0 - 10.0	A vulnerability whose exploitation might be easy, publicly available and of high impact such as gaining total control of the system. Fixing of such vulnerability should be done as urgent as possible

Appendix II: ICT Security Assessment Compliance Criteria

S/N.	ASSESSMENT SCORE	DESCRIPTION
1.	81% - 100% "VERY GOOD"	Getting INFO as highest score, in Common Vulnerability Scoring Systems (CVSS). <i>[i.e. the only vulnerability found is the one that is informational with no risks to an institution].</i>
2.	61% - 80% "GOOD"	Getting LOW as highest score, in Common Vulnerability Scoring Systems (CVSS). <i>[i.e. the most risk vulnerability found, is extremely difficult to exploit or its impact is minimal and the vulnerability may be fixed from time to time as may seem possible].</i>
3.	41% - 60% "ADEQUATE"	Getting MEDIUM as highest score, in Common Vulnerability Scoring Systems (CVSS). <i>[i.e. the most risk vulnerability found, is difficult to exploit and the vulnerability is required to be evaluated and fixed as soon as possible.]</i>
4.	21% - 40% "INADEQUATE"	Getting HIGH as highest score, in Common Vulnerability Scoring Systems (CVSS). <i>[i.e. the most risk vulnerability found, has high confidentiality, integrity and availability impacts that may bring loss to an institution and the exploits might be publicly available and is required to be fixed in priority as immediate as possible.]</i>
5.	0% - 20% "VERY INADEQUATE"	Getting any CRITICAL score in Common Vulnerability Scoring Systems (CVSS). <i>[i.e. finding any vulnerability whose exploitation might be easy, publicly available and of the high impact such as gaining total control of the system and is required to be fixed as urgent as possible]</i>