THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

e-GOVERNMENT AUTHORITY

ISO 9001:2015 Certified

Document Title

Creation of ICT Security Policy – Technical Guide

Document Number

eGA/EXT/ISA/003

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Eng. Benedict B. Ndomba	Director General		14/05/2024

PREFACE

It is of prime importance that Public Institutions implement the necessary controls to ensure that the information and technology assets are protected from all types of threats, whether internal or external, deliberate or accidental, using Institutional ICT Security Policy. ICT Security Policy articulate ICT Security measures, commensurate with ICT Assets Classification to protect ICT Assets and Systems within the Public Institutions ICT environment against authorized use or accidental modification, loss or disclosure. Public Institutions have been using ICT without proper guidance on implementation of ICT security controls that lead to affect the confidentiality, integrity and availability.

In that regard, it was apparent for enactment of the e-Government Act No. 10 of 2019 and its Regulations, 2020, which provide guidance on proper approach for implementing e-Government and establishment of e-Government Authority with mandate of coordinating, promoting and overseeing e-Government implementations as well as enforcing compliance with laws, regulations, standards and guidelines related to e-Government implementations in Public Institutions. Thus, the Authority has formulated this document to establish a technical guide to assist Public Institutions on a proper way of developing and implementing Institutional ICT Security Policy.

In this context, Section 37 (a) of the Act requires Public Institutions to develop and implement Institutional ICT Security Policy and ICT Security Strategy that provide directives for managing ICT security.

Eng. Benedict B. Ndomba
DIRECTOR GENERAL

Table of Contents

1 INTRODUCTION

1.1. Overview

The e-Government Authority (e-GA) was established in 2019 under the e-Government Act, No. 10 of 2019, vested with mandate of coordinating, overseeing, monitoring and promoting e-Government initiatives as well as enforce compliance with e-Government related policies, laws, regulations, standards and guidelines in public institutions. The e-Government Authority is a succeeding institution to e-Government Agency.

ICT Security Policy seeks to protect the confidentiality, integrity, and availability of information and ICT Facilities through the use of established ICT security processes and practices. Since protection of information is expensive, not all controls that are provided in the *ICT Security Samples*, needs to be adopted by institution. The Head of ICT or Head of ICT Security, that is responsible for preparation of ICT Security policy, need to choose only those controls that are applicable to the institution by using risk management procedures.

1.2. Rationale

ICT Security Policy facilitates protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

1.3. Purpose

The purpose of this document is to ensure that ICT Security Policy, is created properly based on ICT Security requirement of the Institution. It provides guidelines for adapting the ICT Security Policy to the needs of Public Institutions. The document provides more technical details and is part of *e-Government Security Architecture (eGA/EXT/ISA/001)* that is directed in "*e-Government Guideline".*

1.4. Scope

This document applies to all Head of ICT/ICT Security who are responsible for the development of ICT Security Policy within their Institutions.

2 THE TECHNICAL GUIDELINES

2.1. Step 1 – ICT Security Risk assessment

2.1.1 Review of ICT Asset Inventory

2.1.1.1. The Head of ICT/ICT Security need to identify all the information assets of and record them in the following categories:

i. Electronic information (e.g., database and data files, test data, backup data, system configuration).

ii. Physical information (e.g., files, user manuals, contracts, system documentation).

2.1.2 Identification of Security Threats

2.1.2.1. The Head of ICT/ICT Security will identify realistic threats to assets using a combination of methods such as conducting a threat modelling exercise and reviewing security incident reports. etc. The main threats that can lead to the compromise of information are provided in the table below:

Ref.	**Description**
External attack	
R1	Carrying out denial of service attacks
R2	Hacking
R3	Undertaking malicious probes or scans
R4	Cracking passwords
R5	Cracking keys
R6	Defacing web sites
R7	Spoofing web sites
R8	Spoofing user identities
R9	Modifying network traffic
R10	Eavesdropping
R11	Distributing computer viruses (including worms)
R12	Introducing Trojan horses

Ref.	Description
R13	Introducing malicious code
R14	Carrying out social engineering
R15	Distributing spam
Internal misuse and abuse	
R16	Gaining authorized access to systems or networks
R17	Changing system privileges without authorization
R18	Changing or adding software without authorization
R19	Modifying or inserting transactions, files or databases without authorization
R20	Misusing systems to cause disruption
R21	Misusing systems to commit fraud
R22	Downloading or sending of inappropriate content
R23	Installing unauthorized software
R24	Disclosing authentication information
R25	Disclosing business information
Loss or theft	
R26	Software piracy
R27	Theft of business information
R28	Theft of identity information (e.g., as a result of Phishing)
R29	Theft of computer equipment
R30	Theft of portable computers and storage devices
R31	Theft of authentication information
R32	Theft of software
Service malfunction	
R33	Malfunction of business application software developed in-house
R34	Malfunction of business application software acquired from a third party
R35	Malfunction of system software
R36	Malfunction of computer/network equipment
Service interruption	
R37	Damage to or loss of computer facilities
R38	Damage to or loss of communications links/services.
R39	Loss of power
R40	Damage to or loss of ancillary equipment
R41	Natural disasters
R42	System overload
Human error	
R43	User errors
R44	IT/network staff errors
Unforeseen effects of changes	
R45	Unforeseen effects of introducing new/upgraded business processes
R46	Unforeseen effect of changes to software
R47	Unforeseen effect of changes to business information

Ref.	Description
R48	Unforeseen effect of changes to computer/communications equipment
R49	Unforeseen effects of organisational changes
R50	Unforeseen effects of changes to user processes or facilities
Legal and regulatory threats	
R51	Breach of data protection or contractual data requirements
R52	Cross border or discovery risk
R53	Breach of EU directive on the use of cookies
R54	Breach of legal and/or regulatory requirements in relation to data retention

2.1.2.2. The Head of ICT/ICT Security will list down the threats associated to the different asset type and asset name as per table below.

Asset Type	Asset Name	Threats identified
<<Physical or electronic>>	**<<As per the naming convention of the institution>>**	**<<Based on the table provided in section 2.1.2.1 above>>**

2.1.3 Identification of Vulnerabilities

2.1.3.1. Vulnerability is an attribute of a secondary asset or a weak/missing control that can be used or exploited in a way, or for a purpose, other than that intended. Typical types and examples of vulnerabilities are shown below:

i. Security weakness in system or software that could be exploited by a hacker;

ii. Single point of failure of a system or service that could lead to loss or unavailability of data;

iii. Site location in an area susceptible to flooding that could lead to loss or unavailability of data.

iv. Susceptibility of electronic media to technical failure that could lead to loss or unavailability of data;

v. Difficult to use or complicated user interface that could lead to human error; and

vi. Cultural issues or territory specific legal or regulatory framework that may prevent the implementation or reduce the effectiveness of some controls.

2.1.3.2. The Head of ICT/ICT Security will list down the vulnerabilities associated with each threat as per table below.

Asset Type	Asset Name	Threats identified	Possible vulnerabilities
<<Physical or electronic>>	**<<As per the naming convention of the institution>>**	**<<Based on the table provided in section 2.1.2.1 above>>**	**<< The potential vulnerabilities leading to each threat is identified>>**

2.1.3.3. The likelihood of such a threat exploiting the vulnerability will be considered making the assumption that no control is currently in place. Likelihood will have a value ranging from 1 – 5 as illustrated in the table below:

Value	Likelihood level
1	0 – 20 % possibility of occurrence (very rarely to occur)
2	21 – 40 % possibility of occurrence (unlikely to occur)
3	41 – 60 % possibility of occurrence (possible to occur)
4	61 – 80 % possibility of occurrence (likely to occur)
5	81 - 100% possibility of occurrence (certain to occur)

2.1.3.4. The Head of ICT/ICT Security will list down the likelihood of each type of threat based on the value provided above.

Asset Type	Asset Name	Threats identified	Possible vulnerabilities	Likelihood
<<Physical or electronic>>	**<<As per the naming convention of the institution>>**	**<<Based on the table provided in section 2.1.2.1 above>>**	**<< The potential vulnerabilities leading to each threat is identified>>**	**<<Based on table above>>**

2.1.3.5. The impact of a vulnerability being exploited by a threat to the business is critical in deciding the level of control required. For example, it will indicate whether there is a need to implement one or many controls to mitigate the risk. The bigger the risk exposure and potential damage to the institution, the more assurance through implementation of controls or other actions will be necessary. Impact will have a value ranging from 1 – 5 as illustrated in the table below:

Value	Impact level
1	Negligible impact to the Public Institution
2	Minor impact to the Public Institution
3	Moderate impact to the Public Institution
4	Major impact to the Public Institution
5	Catastrophic impact to the Public Institution

2.1.3.6. The Head of ICT/ICT Security will list down the impact of each type of threat based on the value provided above.

Asset Type	Asset Name	Threats identified	Possible vulnerabilities	Likelihood	Impact
<<Physical or electronic>>	**<<As per the naming convention of the institution>>**	**<<Based on the table provided in section 2.1.2.1 above>>**	**<< The potential vulnerabilities leading to each threat is identified>>**	**<<Based on table in section 2.1.3.3>>**	**<<Based on table in section 2.1.3.5>>**

2.1.4 Calculation of risks

2.1.4.1. Once the potential impact to the business has been identified and assessed the following formula is used to calculate the Risk Exposure: Risk Exposure = Impact x Likelihood

2.1.4.2. Based on the values provided for each variable, the Risk Exposure will range from 1 (being the least risk exposure) to 25 (being the most critical risk exposure).

2.1.4.3. The Head of ICT/ICT Security will calculate the risk exposure associated to the assets based on the above formula.

Asset Type	Asset Name	Threats identified	Possible vulnerabilities	Likelihood	Impact	Risk Exposure

<<Physical or electronic>>	**<<As per the naming convention of the institution>>**	**<<Based on the table provided in section 2.1.2.1 above>>**	**<< The potential vulnerabilities leading to each threat is identified>>**	**<<Based on table in section 2.1.3.3>>**	**<<Based on table above>>**	**<Based on the above formula?**

2.2. Step 2 – Risk Treatment

2.2.1. The Head of ICT/ICT Security is responsible for establishing and maintaining a Risk Treatment Plan (RTP). The RTP identifies the controls to be implemented in order to mitigate the identified risks.

2.2.2. The Head of ICT/ICT Security will detail the risk treatment plan as per the template below.

Risk Priority	Possible Risk Treatment Option	Risk Rating after treatment	Results Cost benefit Analysis (A- Accept R- Reject)	Person responsible for implementation of option	Time Frame for implementation	How the risk and the treatment will be monitored.
<<Detail out the risk associated to assets based on the risk exposure>	**<<Detail out the possible options to treat the risk as per 10 Government ICT Security Domains >>**	**<<Quantify the risk rating post treatment option>>**	**<< Calculate the cost of the treatment against the benefit>**	**<<Concerned Person>>**	**<<In days or months or year>>**	**<Define evaluation criteria>**

2.2.3. The Head of ICT/ICT Security will use the risk assessment and risk treatment plan to determine security controls as defined in the ICT Security Policy Sample and are applicable to his/her Public Institution.

2.2.4. The RTP is be approved by the management team.

2.3. Step 3 – The ICT Security Policy

2.3.1. The *"ICT Security Policy Sample"* is a sample developed, for purpose of assisting the Head of ICT/Security to develop the ICT Security Policy of the Institution. It should be modified with additions or deletions, to suite Public Institution's need.

2.3.2. The Head of ICT/ICT Security will amend the sample by keeping only those controls deemed necessary to mitigate the identified risks and retain the Sample with only the controls that are applicable to the Institution.

2.3.3. Any security control that is made Mandatory to Public Institution by the Government, through e-Government Policy, e-Government Guidelines or e-Government Standards will be retained in the Sample or added to the Sample.

2.3.4. The document is approved by the highest level of authority at the Institution i.e. Accounting Officer (Head of Institution) or the Board Directors - Chairperson.

2.3.5. The copy of approved ICT Security Policy document is sent to e-GA.

3 IMPLEMENTATION, REVIEW AND ENFORCEMENT

This document shall be:

3.1. Effective upon being reviewed by e-GA Management and signed by the Director General on its first page.

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 Director General.

4 ACRONYMS

4.1. e-GA – e-Government Authority.

4.2. EU – European Union.

4.3. ICT – Information and Communication Technology

4.4. RPT – Risk Treatment Plan.

5 RELATED DOCUMENTS

5.1. e-Government Act, 2019.

5.2. e-Government General Regulations, 2020.

5.3. Tanzania e-Government Strategy 2022.

5.4. Government Cybersecurity Strategy 2022.

5.5. e-Government Guideline, 2017.

5.6. Creation of Government ICT Management Documents - Technical Guide *(eGA/EXT/AVS/003).*

5.7. e-Government Security Architecture – Standards and Technical Guidelines *(eGA/EXT/ISA/001).*

6 DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	Creation of ICT Security Policy – Technical Guide	Creation of Document	Feb 2016
Ver. 1.1	Creation of ICT Security Policy – Technical Guide	Aligning the document with e-Government Act No. 10 of 2019	May 2024

7 ATTACHMENTS

7.1. ICT Security Policy Sample (eGA/EXT/SAM/002)