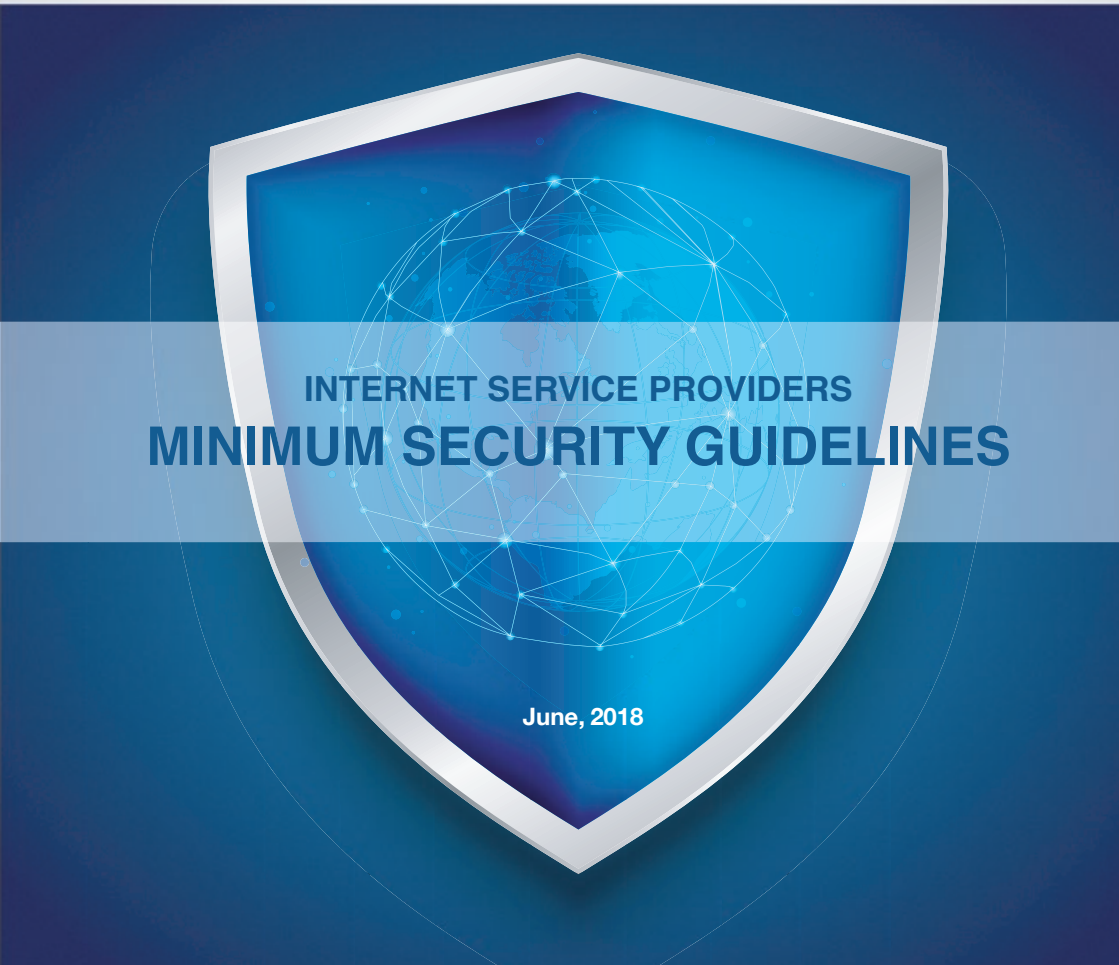
THE UNITED REPUBLIC OF TANZANIA

TANZANIA COMMUNICATIONS REGULATORY AUTHORITY

ISO 9001:2015 CERTIFIED

TZ-CERT

TANZANIA COMPUTER EMERGENCY RESPONSE TEAM



INTERNET SERVICE PROVIDERS

MINIMUM SECURITY GUIDELINES

June, 2018

Abstract

ABSTRACT

As information and communication technologies have continued to expand and converge, the dangers from cyber threats have also significantly increased, triggering wider damage and effects than before. The situation worsens as the society's dependency on ICTs increases.

These guidelines, to be referred to as "the Internet Service Providers' Minimum Security Guidelines", have been made in accordance with Regulation 6 (c) of the Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018 to define a list of operational security requirements for the infrastructure of Internet Service Provider (ISP) networks in their provision of services to users. The goal is to provide network operators a clear, concise way of minimizing security threats to their systems and networks.

By virtue of the position and role played by ISPs in the provision of information and communication technology services in the society, ISPs have a crucial role to play in responding to cyber security incidents. Important as ISPs are in ensuring secure ICT services, it is important that guidelines be in place to ensure that every service provider puts in place secure cyber environment by adhering to minimum security Guidelines that will assist in protecting the users and allow smooth response to cyber security incidents.

Approved by the Tanzania Communication Regulatory Authority, these Guidelines apply to all licensed ISP in Tanzania. It is envisaged that every ISP will ensure her systems and network will meet these Guidelines. While these Guidelines set minimum requirements, ISPs are encouraged to pursue higher security measures.

The Guidelines will be updated at least every six months or as required due to various needs.

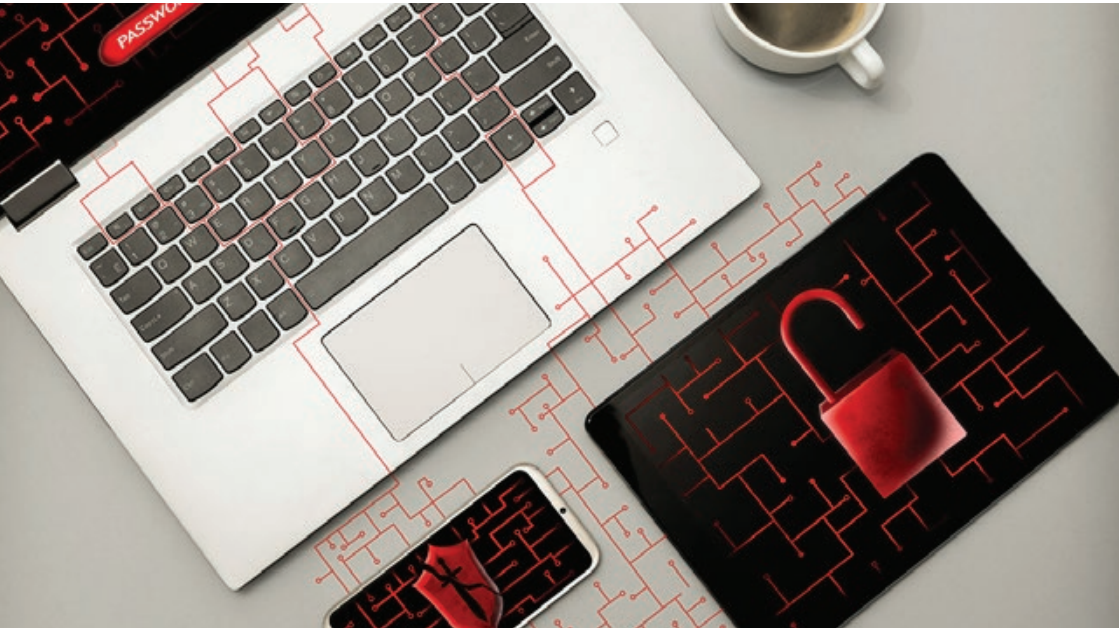


TABLE OF CONTENTS

1. PURPOSE

The purpose of these minimum security guidelines is to ensure that users of Internet Services are properly secured and that the reported incidents can be responded to in an effective and efficient manner that provides enough evidence from Internet Service Providers.

Compliance to these minimum security guidelines will ensure that businesses keep relying on the use of Information and Communication Technologies (ICT) to run their businesses and deliver critical services to their customers.

2. DEFINITIONS

In these guidelines, unless the context otherwise requires:

a. **Authentication,** means to confirm the identity of an entity when that identity is presented;
b. **Authorization,** means to access privileges granted to a user, program, or process or the act of granting those privileges;
c. Dynamic Host Configuration Protocol, abbreviated as DHCP, means a network protocol that enable computer hosts to get assigned IP addresses automatically from a defined range of IP addresses;
d. **Incident a**lso known as Information Security Incident, means single or a series of unwanted or unexpected information security event that have a significant probability of compromising business operations and threatening information security;
e. **Internet Service Provider** abbreviated as **ISP**, means Companies operating in Tanzania, with application service license and providing Internet Services to Tanzanians;
f. **Internet Protocol also known as IP Address**, means a string of number separated by periods (or full colon for IPv6) that identified each host connected to a network;
g. **Log, means** a computer file that records events and activities that occurs when an operating systems runs a particular service.

3. MINIMUM SECURITY GUIDELINES

In providing services to their clients, Internet Service Providers (ISPs) are required to ensure the following set of requirements is implemented:-

3.1 INFORMATION SECURITY GOVERNANCE, RISK AND COMPLIANCE

The ISPs are required to provide the foundations for Information Security management within their organization by implementing the following:-

3.1.1 Information Security Policies

The ISPs shall develop, adopt and maintain appropriate information security policies to ensure secured, reliable and dependable services to their customers.

Management of the ISPs shall ensure that the Information Security Policies are implemented, observed and adhered to in their service provisioning.

3.1.2 Information Security Governance, Risk Management and Compliance Framework

The ISPs shall establish and maintain Information Security Governance framework that establish and mitigate their Information security risks.

The ISPs will establish and maintain the Information Security Governance framework based on nature of their organization and the services offered.

Management of the ISPs shall ensure that the Information Security framework implemented is observed and adhered to in their service provisioning.

3.1.3 Organization's Information Security Roles and Responsibilities

The Internet Service Providers shall ensure they establish and maintain appropriate Information security roles and responsibilities of protecting themselves as well as their customers.

3.1.4 Management of Third Party Services

Where service is delivered through a third party, the ISPs shall ensure these minimum guidelines are observed in the service provided by the third part.

3.2 SECURITY OF SYSTEMS AND FACILITIES

In providing services to their customers, ISPs are required to maintain a secure environment, by ensuring the following:-

3.2.1 Physical Security

ISPs shall establish and maintain reliable physical security of facilities, systems and network infrastructure.

To ensure reliable physical security, ISPs are required to ensure environmental controls are in place to provide protection against theft, fire and other related disasters that may affect their facilities.

ISPs are required to take precautionary measures against natural calamities such as earthquakes, flood and related disaster.

3.2.2 Access Control

ISPs shall establish and maintain the logical access control to the systems and network infrastructure.

ISPs shall ensure mechanisms to identify and authenticate each of its users before providing services.

3.2.3 Audit and Accountability

ISPs shall implement a mechanism to provide auditability and accountability to the activity performed in their systems and networks. In implementing this mechanism, the ISP shall keep the logs for the minimum of six (6) months.

The logs that must be retained shall include but not be limited to:

i. DHCP assignments;
ii. Access and authentication logs to systems and network devices;
iii. Services logs such as web services logs, database logs.

3.2.4 Security of Systems and Network Infrastructure

ISPs shall identify malicious traffic destined to their systems and adopt technical measures to filter such traffic.

ISPs shall ensure appropriate privacy of the customer's information is maintained.

ISPs shall ensure they detect and prevent propagation of incorrect routing information as well as spoofed IP source addresses.

3.3 INCIDENT MANAGEMENT AND RESPONSE

ISPs are required to ensure the information security incidents reported are responded effectively and efficiently by doing the following:-

3.3.1 Incident Response Procedures

ISPs shall establish, adopt and maintain policies, processes and procedures for managing cyber security incidents within their organizations.

The policies, processes and procedures shall, among other things, cover incident reporting, response and communication with customers.

The policies shall provide for, among other things, the escalation procedures and the appropriate roles and responsibilities in responding to the incidents.

3.3.2 Incident Detection Capabilities

ISPs shall build incident detection capabilities by deploying security measures that can detect security incident.

ISPs shall report to Tanzania Computer Emergency Response Team all information Security Incidents detected.

The incidents shall include but not be limited to:-

i. Intrusions to the ISPs network;
ii. Breach of customer's data;
iii. Denial of Service and Distributed Denial of Service Attacks;
iv. Malware outbreaks;
v. Spam related incidents;
vi. Phishing attacks;
vii. Spoofing related attacks;
viii. Web defacement.

Where the incidents concern the privacy and security of the customers, the ISPs shall inform the customer about the incidents, measures taken to handle the incidents and measures the customer need to take to protect themselves.

3.4 INFORMATION SECURITY TESTING AND AUDITING

ISPs are required to maintain a secure environment for delivering services to customers by ensuring the following:-

3.4.1 Contingency Plans Testing

ISPs shall perform contingency plans testing at least once a year in order to ensure the prepared contingency plans have been appropriately implemented to provide continuity of the ISPs services to customers.

3.4.2 Security Assessments

ISPs shall perform independent information security assessments at least once a year to ensure they continue to provide secure and reliable services to the customers.

The information security assessment shall, among other things, cover the operating procedures, physical security and systems security.

3.4.3 Compliance Monitoring and Audit

ISPs shall perform an annual self or third party audit to verify the organization's compliance to their information security framework.

The auditor shall also verify the relevance of the Information Security Framework in protecting the ISP and their customers

3.5 BUSINESS CONTINUITY MANAGEMENT

To minimize the risks that may be suffered by the customers and ensure business continuity, the ISPs shall be required to perform the following:-

3.5.1 Business Continuity Strategy and Contingency plan

ISPs shall develop, maintain and adopt comprehensive business continuity plans to ensure continuity of reliable and dependable services to their customers.

3.5.2 Disaster Recovery capability

In implementing and adopting their business continuity plans, ISPs shall implement disaster recovery capabilities for restoring services after the disaster.

4. CONCLUSION

To provide secure and reliable services to the customers, the ISPs are required to implement these mandatory minimum guidelines.

It is to be noted that, these are minimum guidelines; and the ISPs are encouraged to implement advanced standards/framework to protect their customers such as implementation of ISO 27000 Information Systems Security Management.

The Authority may, from time to time, carry out regulatory checks to ensure compliance to these guidelines.

ABOUT TZ-CERT

Tanzania Computer Emergency Response Team (TZ-CERT) was established under section 124 of the Electronic and Postal Act (EPOCA) no 3/2010 within the structure of Tanzania Communication Regulatory Authority (TCRA) as the trusted focal point of contact for coordinating response to cyber security incidents at the national level. It cooperates with regional and international bodies involved in the management of cyber security incidents.

Vision: To be a globally trusted hub for handling Cyber Security Incidents.

Mission: To improve and support the Nation's Cyber Security posture, coordinate information sharing and proactively manage Cyber risk while enhancing Constituencies commitment.

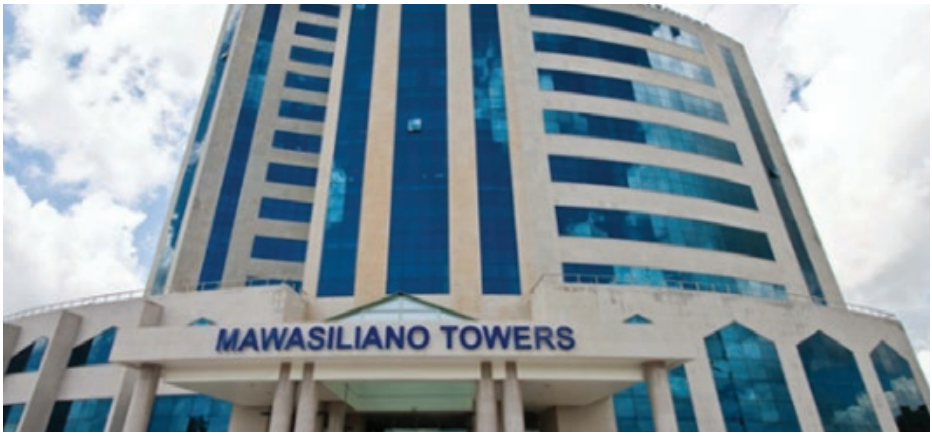
Services:

TZ-CERT extended services to its constituencies includes;

1. Cyber Security Incident Handling,
2. Cyber Security Awareness Programs,
3. Cyber Security Capacity Building Programs,
4. Cyber Security Alert, Warnings and Announcements,
5. Vulnerabilities Handling and Penetration Testing,
6. Digital Forensic Investigation.

TZ-CERT Constituents (Customers);

• **Government** – Ministries, Departments, Agencies, Local Government and Authorities (MDAs LGAs), • **Commercial**;	• **Academia** – Public and private learning institutions; • **Finance and Banking institutions**; • and **Vendors**	• **Critical ICT Infrastructure (CII);** • **Defence and Security** – Law enforcement Agencies;



CONTACT:

TANZANIA COMPUTER EMERGENCY RESPONSE TEAM (TZ-CERT)
Mawasiliano Towers
20 Sam Nujoma Road
P.O. Box 474
14414, Dar Es Salaam

Tel:	+255 22 2199760-9
	+255 22 2412011-2
Mob:	+255 784 558270-1
Fax:	+255 22 2412 038
Email:	info@tzcert.go.tz
Website:	https://www.tzcert.go.tz

PGP Key id: EF916FCAEED630F6
PGP Key Fingerprint: 0A1C CF48 D623 9BE7 676B 4C03 EF91 6FCA EED6 30F6

TZ-CERT

TANZANIA COMPUTER EMERGENCY RESPONSE TEAM

https://www.tzcert.go.tz

tzcert

tz_cert

tz_cert

Issued by:

The Director General
Tanzania Communication Regulatory Authority (TCRA)
Mawasiliano Towers
20 Sam Nujoma Road
P.O. Box 474
14414, Dar Es Salaam

Tel: +255 22 2199760-9
+255 22 2412011-2
Mob: +255 784 558270-1
Fax: +255 22 2412 038
E-mail: dg@tcra.go.tz
barua@tcra.go.tz