GOVERNMENT NOTICE NO. 570 published on 11/8/2023

THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT,
(CAP. 306)

REGULATIONS

(Made under section 165)

THE ELECTRONIC AND POSTAL COMMUNICATIONS (COMPUTER EMERGENCY RESPONSE TEAM) (AMENDMENT) REGULATIONS, 2023

ARRANGEMENT OF REGULATIONS

THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT,
(CAP. 306)

REGULATIONS

(Made under section 165)

THE ELECTRONIC AND POSTAL COMMUNICATIONS (COMPUTER EMERGENCY RESPONSE TEAM) (AMENDMENT) REGULATIONS, 2023

Citation

GN. No. 60 of 2018

1. These Regulations may be cited as the Electronic and Postal Communications (Computer Emergency Response Team) (Amendment) Regulations, 2023 and shall be read as one with the Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018 hereinafter referred to as "the principal Regulations".

Amendment of regulation 3

2. The principal Regulations are amended in regulation 3, by-

(a) deleting the definition of the term "WHOIS database"; and

(b) adding in their appropriate alphabetical order the following new definitions:

"cybersecurity service" means cybersecurity consultancy services including penetration testing or managing security operation centres and any other cybersecurity related services;

"cybersecurity tool" means system, equipment, software and other technology specifically designed or modified to develop, generate, command and control

or deliver intrusion software or forensic devices;

"security operation centre" means a centre established for the purpose of conducting continuous monitoring and improving of an organisation's security posture while preventing, detecting, analysing and responding to cybersecurity incidents;

"security penetration testing" means a method of gaining confidence in an IT systems security by attempting to breach some or all of that system's security using tools and technique;".

Amendment of regulation 5

3. The principal Regulations are amended in regulation 5-

(a) in subregulation (3), by-

(i) deleting paragraph (h) and substituting for it the following:

"(h) the manager of National CERT who shall be the Secretary;

(i) one representative from academic, research and development institution."

(ii) renaming paragraph (i) as paragraph (j); and

(b) adding immediately after subregulation (3) the following:

"(4) Members of the Technical Advisory Committee shall possess-

(a) a minimum qualification of a degree or its equivalent from a recognised higher education institution in computer science, telecommunication, computer engineering, software engineering, information security or any other related field;

(b) a cybersecurity professional

certificate from a recognised institution; and

(c) a minimum experience of five years in the cybersecurity industry.

(5) The tenure of office of the Technical Advisory Committee members shall be three years from the date of appointment and may be eligible for reappointment for one further term."

Amendment of regulation 7

4. The principal Regulations are amended in regulation 7 by-

(a) adding immediately after paragraph (g) the following:

"(h) engage licensed security penetration testers;

(i) perform independent information security assessments at least once a year to know and apply remedial measures against its security weaknesses;

(j) share key findings of the security assessment performed to National CERT as soon as possible;

(k) protect organisation's domain names by applying secure protocols like Hypertext Transfer Protocol Secure (HTTPS) and Domain Name System Security Extensions (DNSSEC);

(l) establish, adopt and maintain policies, processes and procedures for managing cybersecurity incidents within their organisation;

(m) implement disaster recovery plan for restoring services after cybersecurity incident or disaster;

(n) create and update cybersecurity incidents register;"; and

(b) renaming paragraphs (h) and (i) as paragraphs (o) and (p), respectively.

Amendment of regulation 8

5. The principal Regulations are amended in regulation 8, by -

(a) deleting the words "WHOIS database" appearing in paragraph (e) and substituting for them the word "information";

(b) deleting paragraph (f);

(c) renaming paragraphs (g), (h), (i), (j), (k) and (l) as paragraphs (f), (g), (h), (i), (j) and (k), respectively; and

(d) deleting paragraph (j) as renamed and substituting for it the following:

"(j) retain the contents of user's access logs including Dynamic Host Configuration Protocol (DHCP) assignment logs, traffic or routing data, for a minimum period of six months or as may be determined by the Authority;".

Amendment of regulation 9

6. The principal Regulations are amended in regulation 9 by-

(a) adding immediately after subregulation (1), the following:

"(2) A national application service licensee shall-

(a) maintain cybersecurity personnel for cyber incident response;

(b) perform vulnerability assessment and penetration testing of their network, systems and applications at least twice a year to ensure the highest levels of security, reliability, confidentiality and consumer protection;

(c) perform security testing prior to granting approval for any system or application to move into production;

(d) fix the identified vulnerability by applying patches or secure configuration;

(e) ensure real-time monitoring of systems and networks for security breaches and intrusions that may affect their network, systems and consumers, as well as reporting to the Authority of any breaches and intrusions;
(f) continue testing, intrusion filtering and monitoring of their core networks infrastructure and licensed frequency bands to ensure that there is no unauthorised access, disruption or use;
(g) implement the security advisory issued by the Authority and report back to the Authority its implementation status in quarterly basis;
(h) take all required security measures to guarantee the confidentiality, integrity and availability of their network, systems and services for the entire duration of the license;
(i) where the licensee is a mobile network operator, put access level controls to systems, validate and ensure that only vetted and authorised persons are able to have access to or provide subscribers information;
(j) put in place documented security policies and procedures to mitigate all known risks associated with the services offered to avoid damage to, or failure of systems which may cause interruption of subscribers' services or make subscribers suffer from any associated losses;
(k) conduct cyber security risk assessment at least twice a year and maintain an updated risk register;
(l) conduct cyber security awareness to their subscribers and report to the Authority in quarterly basis; and
(m) monitor and comply with security standards and guidelines provided by the Authority to

maintain secured networks, systems and services."; and

(b) renumbering subregulation (2) as subregulation (3)

Amendment of regulation 10

7. The principal Regulations are amended in regulation 10, by-

(a) adding immediately after paragraph (a) the following:

"(b) create and update cybersecurity incident register;

(c) coordinate the response of the cybersecurity incidents at sectorial level and collaborate with the national CERT in response to such incidents;

(d) strengthen sectorial prevention capability against existing cybersecurity threats by monitoring and applying remedial measures against cyber-attacks;

(e) raise awareness and enhance technical capacity in the area of cybersecurity within the specific sector;

(f) conduct periodic independent cyber security assessment covering the internal and external level of the organisation;

(g) maintain an accurate and up-to-date asset inventory of all the information assets that includes all relevant details to facilitate efficient protection of the information assets;

(h) establish and implement an appropriate cybersecurity risk assessment approach to identify, analyse and evaluate the risks to protect the information assets;

(i) establish and implement an appropriate cybersecurity risk treatment and monitoring approach to manage the identified risks and monitor the treatment plans;

(j) protect the networks operated by the

organisation from malicious activities and ensure the networks resilience against cyber threats;

(k) monitor and protect the event logs of the information assets and report suspicious events to the National CERT;"; and

(b) renaming paragraphs (b) and (c) as paragraphs (l) and (m), respectively.

Amendment of regulation 11

8. The principal Regulations are amended by deleting regulation 11 and substituting for it the following:

"Obligations of users of computer and equipment with data processing capabilities

11. A user of any computer or equipment with data processing capability shall-

(a) not attempt to gain unathorised access to a computer or intentionally or knowingly cause loss or damage to the public or any person destroy or delete or alter any information in the computer resources or diminish its value or utility or affect it injuriously by any means;

(b) perform vulnerability assessment and penetration testing of their network, systems and applications to ensure the highest levels of security, reliability, confidentiality;

(c) perform security testing prior to granting approval for any system or application to move into production;

(d) fix the identified vulnerability by applying patches or secure configuration;

(e) ensure real-time monitoring of systems and networks for security breaches and intrusions that may affect their network, systems and consumers; as well as reporting to the

Authority of any breaches and intrusions;

(f) implement the security advisory issued by the Authority from time to time and report back to the Authority its implementation status in quarter basis;

(g) put in place documented security policies and procedures to mitigate all known risks associated with the services offered to avoid damage to, or failure of systems;

(h) conduct cyber security awareness to their customers; and

(i) monitor and comply with security standards and guidelines provided by the Authority to maintain secured networks, systems and services.".

Addition of Part III

9. The principal Regulations are amended by-

(a) adding immediately after Part II, the following new Part:

"PART III
CYBER SECURITY SERVICE

Licensing of cybersecurity service providers

12.-(1) A person who intends to provide cybersecurity services within the United Republic shall obtain a licence from the Authority.

(2) A person referred to under subregulation (1) shall be required to possess eligible professional certificate from a recognised institution.

(3) An application for licence shall be in a prescribed form accompanied by the following:

(a) in case of an individual-
  (i) certified copy of the national identification;
  (ii) applicant contact which include residential address and, if different, the applicant's correspondence address;
  (iii) certified evidence of applicant's qualifications relating to cyber security services for which license is sought;
  (iv) certified evidence of applicant's experience, if any, relating to cybersecurity services for which license is sought;
  (v) information on whether the applicant has been convicted of an offence involving fraud, dishonest or moral turpitude or an offence the conviction of which involves finding that the applicant has acted fraudulently or dishonestly;
  (vi) provide any other information as may be specified by the Authority; and
  (vii) proof of payment of fees as prescribed in the Schedule;
(b) in case of business entity-
  (i) name of the entity;
  (ii) certificate of

registration or incorporation;

(iii) address including phone number and email address;

(iv) physical address of the registered principal place of business;

(v) certified copy of director's national identification;

(vi) information on whether the applicant has been convicted or anyhow involve in civil proceeding involving fraud, dishonest or breach of fiduciary duty on the part of the applicant;

(vii) certified information relating to applicant's director or employees or proposed employee's qualification relating to cybersecurity services, provided that, the employees shall have supervisory responsibility in the provision of cybersecurity services;

(viii) information relating to applicant's director or employees or proposed employee's experience relating to cyber

security services, provided that, the employee shall have supervisory responsibility in provision of cyber security services; and

(ix) proof of payment of fees as prescribed in the Schedule to these Regulations.

Duties and obligations of cyber security service providers

13. Cybersecurity service provider shall-

(a) not make any false representation in the course of advertising or providing its cybersecurity services;

(b) comply with all applicable laws in the course of providing its cybersecurity service and all obligations relating to confidentiality and data protection;

(c) exercise due care and skill, and act with honesty and integrity in the course of and after providing its penetration testing service;

(d) not act where there is a conflict between his interests and that of the person procuring or receiving the cybersecurity service;

(e) not collect, use or disclose information for other purposes, unless appropriate written consent has been obtained from the person to whom the information relates, or such collection, use or disclosure is

lawfully required by any court or lawfully required or allowed under law;

(f) provide information concerning or relating to its cybersecurity service upon request, and within the timeframes specified by the Authority; and

(g) notify the Authority of any change or inaccuracy in his licence related information and particulars that he or his key employees provided to the Authority, include, but are not limited to-

(i) change of key employee when ceases to work with the company;

(ii) changes to or inaccuracies in the licensee's or its key employees' names, designations, addresses and contact particulars;

(iii) criminal convictions or civil judgments entered against the licensee or its key employees for offences or proceedings involving fraud, dishonesty, breach of fiduciary duty, or moral turpitude, or any offences; or

(iv) where the licensee has been declared bankrupt or has gone into compulsory or voluntary liquidation other than for the purpose of merger or rebuilding.

Publication of cyber security service providers

14. The Authority shall publish in its website the list of entities and individuals licensed to provide cybersecurity services in Tanzania.

Importation, distribution, supply and sell of cybersecurity tools

15. Save for law enforcement organs, a person shall not acquire, import, distribute, supply, or sell cybersecurity tools without obtaining an approval from the Authority:

Provided that, any tool approved under section 83 of the Act shall not be subjected to the requirement of this regulation.";

(b) designating Part III as Part IV; and

(c) renumbering regulations 12, 13, and 14 as regulations 16, 17 and 18 respectively.

Addition of Schedule

11. The principal Regulations are amended by adding immediately after regulation 18 as renumbered the following Schedule:

SCHEDULE

(Made under regulation 12(3))

CYBER SECURITY SERVICES LICENCE FEES AND DURATION

Applicant	Application fee (US Dollars or its equivalent in Tanzanian Shillings)	Registration fee (US Dollars or its equivalent in Tanzanian Shillings)	Annual Maintenance Fees (US Dollars or its equivalent in Tanzanian Shillings) (payable one year after registration)	Duration of licence (Years)
Individual	10	500	500	1
Business Entity	50	2,000	2,000	1

”

Dodoma,
29th July, 2023

NAPE M. NNAUYE
Minister for Information, Communications and Information Technology