GOVERNMENT NOTICE No. 60 published on 23/02/2018

THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT
(CAP. 306)

_____

REGULATIONS

_____

(Made under section 165)

_____

THE ELECTRONIC AND POSTAL COMMUNICATIONS (COMPUTER EMERGENCY RESPONSE TEAM) REGULATIONS, 2018

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) REGULATIONS, 208

PART I
PRELIMINARY PROVISIONS

Citation

1. These Regulations may be cited as the Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018.

Application

2. These Regulations shall apply to electronic communication operators, internet service providers and users.

Interpretation

3. In these Regulations, unless the context otherwise requires:-

Cap.306

"Act" means the Electronic and Postal Communications Act;

"application service licensee" means a person issued with an application service licence by the Authority;

Cap.172

"Authority" means the Tanzania Communications Regulatory Authority established under the Tanzania Communications Regulatory Act;

"Computer Emergency Response Team" (CERT) means a team that responds to computer security incidents by providing necessary services to solve or support their resolutions, and tries to prevent any computer related security incidents to a defined constituency;

"CERT service" means proactive or reactive services aimed at prevention or resolution of computer related security incidents;

"constituency" means people or organizations that the CERT is designed to serve or support;

"cyber security" means protecting information or any form of digital asset stored in computer, computer devices, communication devices or digital memory device from unauthorised access, use, disclosure, disruption, modification or destruction;

"computer security" means administrative and technical measure to attain a secure computing environment free of risk or danger by mitigating vulnerabilities associated with usage of computer or any device with data processing capabilities;

"filtering" means prevention of submission, transfer or delivery of unwanted email messages, malicious software or other unwanted content;

"information security" means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, modified by those who are entitled to do so, and that information system can be used by those who are entitled to use them;

"malicious traffic" means traffic that may endanger or impact the proper functioning of the computer system or undermine the security of the information in a computer system;

"National CERT" means a computer emergency response team established under section 124 of the Act;

"service provider" means a person licensed to provide electronic communication services;

"security incident" means the act of violating an explicit or implied security policy, which include attempts to gain unauthorised access to a system or its data, denial of service or unwanted disruptions, unauthorised use of a system for processing or storing data and to make changes in system hardware or software without the consent of the owner;

"significant security breach" means any circumstance or event having an adverse effect on security of constituency systems and network such as Denial of Service(DoS) or Distributed Denial of Service (DDoS) attacks, Malware attacks, Botnet attacks or other related events;

"stakeholders" means an individual, group or organization from within or outside the country with an interest in the success of the National CERT and its mission;

"subscriber" means a person who has entered into an agreement concerning the provision of a communication service or value added service; and

"WHOIS database" means a searchable database that provides public access to information about domain names, Internet Protocol addresses, Autonomous System Number and their associated information maintained by the registry.

PART II
THE COMPUTER EMERGENCY RESPONSE TEAM AND CONSTITUENCIES

Power of the Authority

4. The Authority shall develop and maintain a comprehensive set of rules and guidelines for effective operations of the National CERT.

Establishment and composition of the national CERT

5.-(1) The National CERT shall be established as a unit within the structure of the Authority.

(2) There shall be established a Technical Advisory Committee which shall advise the Authority on the operations of the National CERT.

(3) The Technical Advisory Committee shall have a maximum of twelve members appointed by the Minister composed of the following:-

(a) a Chairman;
(b) two representatives from the Authority;
(c) a representative from financial service regulator;

(d) a representative from the Ministry responsible for communications;
(e) two representatives from Government Agencies responsible for national security and law enforcement;
(f) a representative from key Government Agency responsible for coordination, oversight and provision of e-Government service;
(g) a representatives from the communication services providers;
(h) the head of National CERT who shall be the Secretary to the Technical Advisory Committee; one member from academic, research and development institution; and
(i) a representative from private sector.

Responsibility of national CERT

6. The National CERT shall:-

(a) establish and maintain trust with its stakeholders, including regional and international entities that are involved in management of cyber security incidents;
(b) maintain a trusted National focal Point of Contact (PoC) within and beyond the national boarders that responds to cyber security incidents;
(c) develop, maintain, adopt, communicate and enforce cyber security standards, minimum security specifications and security requirement to its constituencies;
(d) define and communicate CERT services to its constituencies;
(e) establish and maintain a database of constituents' profile for efficient service delivery and support;
(f) devise, define and develop communication approach and mechanisms to be used to share and disseminate information to constituents, service providers, stakeholders and enable them to share any such information;
(g) develop and deliver a set of crucial reactive and proactive services to the constituency;
(h) forecast and broadcast alerts on cyber security incidents;

(i) issue guidelines, advisory and vulnerability notes relating to information on security practices, procedures, prevention, response and reporting of cyber threats;
(j) coordinate the response of cyber security incidents at a national level, and collaborate with other relevant organizations in response to such incidents;
(k) raise awareness and enhance technical capacity in the area of cyber security;
(l) escalate the security and other related incidences to national security and law enforcement agencies for further action, including prosecution;
(m) perform on demand and scheduled security assessment to critical ICT infrastructure and critical services in order to assess their vulnerabilities to cyber security threats;
(n) provide second opinion for the forensic investigation requested by law enforcement agencies;
(o) coordinate other sectoral specific CERTs, including Government Network CERT established under their respective legislations and to act as a bridge between them and international CERTs; and
(p) carry out such other functions related to cybercrimes as may be prescribed by the Authority.
(q) handle and monitor cybersecurity incidents;
(r) strengthen constituencies' defence capability against existing cyber security threats by monitoring and blocking cyber-attacks.
(s) proactively provide early warning on eminent cybersecurity incidents;
(t) participate on development and implementation of Cyber Security incident simulation scenarios and programs;
(u) monitor and manage Cyber threats and vulnerabilities;
(v) develop National roadmap for improving Cyber Security awareness;
(w) create fora to promote information sharing on Cyber Security;
(x) create and update Cyber Security incidents register;
(y) assess incidents and implement remedial measures;

(z) detect and disseminate information related to Cybersecurity incidents;

Requirements to the Constituencies

7. The Constituencies shall have the duty to:-

(a) maintain a secure environment for their organizations, Internet connectivity and internal network for their users by maintaining up-dated systems that have a protection mechanism against information and computer security threats;

(b) maintain an organization's Information Communication Technology and cyber security policy for information and computer security;

(c) maintain a trusted focal point of contact with authority in cyber security issues within the organizations, who shall communicate with national CERT and other members of constituents in an effective and timely manner;

(d) submit information related to focal point of contact to national CERT in a specified format;

(e) maintain a good working relationship with their service providers for an efficient and timely communication response;

(f) notify the national CERT of any significant security breach to the constituency systems or networks and measures undertaken to resolve the security breach;

(g) develop internal information awareness programmes for their information and computer users;

(h) comply with security standards, guidelines, minimum security specifications, minimum requirements recommended by the national CERT or service providers for securing their information and computer systems or in response to threats or identified vulnerabilities; and

(i) comply with national CERT requirements by maintaining updated and correct profile for the constituency database.

Obligations of service providers on cyber security

8. The Service Providers shall have the following obligations in relation to cyber security to:-

(a) provide a secure environment for the connectivity of their subscriber base by maintaining updated systems that have a protection mechanism against information security threats;

(b) provide an effective and timely response to the National CERT and support to their subscriber base in a notification on significant information or computer security threats as per guidelines issued by national CERT;

(c) notify the national CERT of any significant security breach to the constituency systems or networks and measures undertaken to prevent reoccurrence of the threat;

(d) collaborate and cooperate with the national CERT in incident handling process so as to effectively solve or support their resolution;

(e) maintain an up-to-date WHOIS database of the IP address block assigned to their customers, which shall apply to each of their IP address assignment;

(f) update the database of IP address block and submit to the national CERT on monthly basis;

(g) disconnect a subscriber or its services from the respective communication network, if proven by the national CERT that the respective subscriber endanger the security of the cyber space, such disconnection shall be carried out in accordance with the predefined guidelines issued by the national CERT;

(h) establish and maintain internal processes to handle various cyber security attacks that may endanger the

security of the cyber space or the usability of the communication services and the communication network;

(i) publish into their website an appropriate notification of the measures taken and any effects they may have on the use of that service after having combated the threat or removed a disruption;

(j) submit detailed periodic reports of incidences and threats on notification as it may be stipulated by the national CERT which shall**,** where possible, give an account of the causes of the threat, number of subscribers affected, other harmful consequences caused by the incident and repair time;

(k) retain the contents of user's access logs, traffic or routing data, for a minimum period of twelve months or as shall be determined by the Authority from time to time; and

(l) abide by the CERT guidelines and directives as prescribed by the Authority from time to time.

Obligation of constituencies and service providers on information security and functionality of services

9.-(1) The Constituencies and application service licensees shall, in the issues of information security and functionality of services be required to:-

(a) maintain up to date and reliable mechanisms for identifying the sources of malicious traffic from the incoming or outgoing traffic; and

(b) filter such traffic that it has identified as malicious traffic.

(2) For the purpose of this regulation "services" includes email, Domain Name Service (DNS), website, public fora and social networks.

Obligation of sector specific CERT

10. The sectoral specific CERT shall be required to:

(a) notify the national CERT on a significant information or computer security threats on their domain;

(b) cooperate with law enforcement and regulatory agencies investigating cybercrime or other illegal activity; and
(c) abide by the CERT guidelines and directives as prescribed by the Authority from time to time.

Obligations of users of computers and equipment with data processing capabilities

11. Any user of any computer or equipment with data processing capability shall not attempt to secure unauthorised 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.

PART III
GENERAL PROVISIONS

Quality and reliability of service

12.-(1) The service provider shall continuously monitor the quality and reliability of the general operations related to the services it provides to its subscriber base.

(2) The constituents shall continuously monitor the quality and reliability of the general operations related to the services it receives from service providers.

(3) The service providers shall have the appropriate mechanisms to detect major problems affecting the functionality of services it provides and for reacting to them.

(4) The service providers shall continuously monitor, compile and submit the statistics below, on quarterly basis, to the national CERT on:-

(a) the volume of traffic identified, marked and filtered as malicious;

(b) significant exceptional situations affecting the usability of services; and

(c) faults found in individual subscriber base.

(5) For the purpose of this regulation, "fault" means any security flaw or security breach automatically detected by services provider from the subscriber such as:-

(a) spreading spam;
(b) phishing;
(c) malicious code;
(d) Botnet.

Compliance and penalty

13.-(1) Any person who contravenes any of these Regulations commits an offence and shall, on conviction, be liable to a fine prescribed under the Act.

(2) Notwithstanding sub regulation (1), where a person commits an offence under these Regulations, the Director General may, where such person admits in writing compound such offence by collecting from that person a sum of money not exceeding the amount of the fine prescribed for the offence.

Revocation of G.N No.419 of 2011

14. The Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2011 are hereby revoked.

Dar es Salaam,
30th January, 2018

MAKAME M. MBARAWA,
Minister for Works, Transport and Communications