GOVERNMENT NOTICE NO. 419 published on 9/12/2011

THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT

(CAP.306)

_____

REGULATIONS

_____

THE ELECTRONIC AND POSTAL COMMUNICATIONS (COMPUTER EMERGENCY RESPONSE TEAM) REGULATIONS, 2011

ARRANGEMENT OF REGULATIONS

THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT

(CAP.306)

_____

REGULATIONS

_____

THE ELECTRONIC AND POSTAL COMMUNICATIONS (COMPUTER EMERGENCY RESPONSE TEAM) REGULATIONS, 2011

PART I
PRELIMINARY PROVISIONS

Citation

1. These Regulations may be cited as the Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2011.

Application

2. These Regulations shall apply to all 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 legal entity issued 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 from risk or danger by mitigating the vulnerabilities associated with usage of computer or any device with data processing capabilities;

"filtering" means prevention of submission, transfer or delivery of email messages, removal of malware endangering information security messages, or other similar technical measures;

"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 the functioning of internet service or may, in essence, weaken the usability of internet;

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

"service provider" means a legal entity holding application service licence;

"security incident" means the act of violating an explicit or implied security policy, which includes 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;

"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 body corporate or a natural person who has entered into an agreement concerning the provision of a communication service or value added service;

"WHOIS database" means a searchable database that provides public access to information about domain names and contacts associated with them and maintained by registrars who follow a query or response protocol.

PART II
THE COMPUTER EMERGENCY RESPONSE TEAM AND CONSTITUENCIES

Power of the Authority

4.-(1) The Authority shall appoint members from stakeholders to form a steering committee for the establishment of the National CERT.

(2) 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 within the structure of the Authority.

(2) The composition of the National CERT shall include members from the public and private sector with interest in Network and Information security.

(3) The National CERT shall consist of a Technical Advisory Committee to be chaired by the Authority.

(4) The Technical Advisory Committee shall have a maximum of twelve members appointed by the Authority

which shall be comprised of the following-

(a) three representatives from the Authority;
(b) a representative from the Ministry responsible for ICTs;
(c) two representatives from key Government Agencies responsible for National Security and Law enforcement;
(d) a representative of the Constituencies;
(e) two representatives from the Service Providers; and
(f) a maximum of three members co-opted by merit, as may be determined by the Authority.

Responsibility of National CERT

6. The National CERT shall be required to-

(a) establish and maintain operational and relational mechanism so as to maintain trust with its stakeholders including both regional and international entities that are involved in the 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 and communicate cyber security procedures and standards to its constituencies;
(d) define and communicate CERT services to its constituencies;
(e) provide quality support and services to its defined constituencies in a timely and effective manner;
(f) establish and maintain a database of constituents' profile for efficient service delivery and support;
(g) develop and maintain a website for public and

closed members, mailing list and other communication channels for efficient communication;

(h) develop and define communication approach and information sharing among the constituents, service providers and stakeholders;

(i) develop and deliver a set of crucial reactive services to the public for continuous awareness and knowledge sharing;

(j) forecast and broadcast alerts on cyber security incidents;

(k) take Emergency measures for handling cyber security incidents;

(l) issue guidelines, advisory and vulnerability notes and relating to information on security practices, procedures, prevention, response and reporting of cyber threats;

(m) develop a collaborative relationship with other CERT type organisations and associates;

(n) raise awareness and provide training to sectoral security CERTs;

(o) escalate the security and other related incidences to national security and law enforcement agencies for further action including prosecution;

(p) perform on demand and scheduled security audits to critical ICT infrastructure and critical services in order to assess their vulnerabilities to cyber security threats;

(q) such other functions related to cyber crimes as may be prescribed by the Authority; and

(r) coordinate other sectoral specific CERTs including Government Network CERT established under their respective legislations

and to as a bridge between them and International CERTs.

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 contacts for the organisation who shall communicate with National CERT and Members of closed constituents mailing list in an effective and timely manner;

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

(e) notify the National CERT of significant information or computer security threats that come to their attention. The notification shall include measures undertaken, if any;

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

(g) comply with the minimum standards, updates or guidelines advised or recommended by the National CERT or service providers for securing their information and computer systems or in response to threats or vulnerabilities came into notice;

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 up dated systems that have a protection mechanism against information security threats;

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

(c) notify the National CERT of significant information or computer security threats that come to their attention. The notification shall include 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 WHOIS database of the IP address block if assigned to self and contact information regarding address and spaces allocated to the respective subscriber base;

(f) disconnect a subscriber or its services from the respective communication network, if it has been proved that a subscription endangers the information security or usability of a communication service; such disconnection and reconnection of a subscriber shall be carried out in accordance with the predefined processes and guidelines;

(g) establish and maintain internal instructions and operation models for denial of service attacks

and other events that may endanger the information security or usability of communications services and communication network for service provider who provide services through backbone network;

(h) 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;

(i) 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;

(j) 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

(k) 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;

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

(c) describe and communicate the general principles of filtering incoming and outgoing

traffic to customers;

(2) For the purpose of this regulation "services" includes email, Domain Name Service (DNS), website, public forums 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 all law enforcement and regulatory agencies investigating cybercrime or other illegal activity;

(c) Abide by the CERT guidelines and directives as prescribed by the Authority from time to time.

Obligations of users of computers and phones with data processing capabilities

11. Any user of any computer or phone 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 and compile submission of below statistics 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.

Compliance and Penalty

13. Any person, contravening any of these Regulations, commits an offence and shall be liable to a fine not less than five hundred thousand Tanzania shillings or to imprisonment for a term not exceeding three months or both.

Dar es Salaam
29th November, 2011

MAKAME M. MBARAWA
Minister for Communication, Science and Technologies