STATUTORY INSTRUMENTS
SUPPLEMENT No. 30 8h November, 2019

STATUTORY INSTRUMENTS SUPPLEMENT

to The Uganda Gazette No. 57, Volume CXII, dated 8th November, 2019

Printed by UPPC, Entebbe, by Order of the Government.

STATUTORY INSTRUMENTS

2019 No. 81.

THE UGANDA COMMUNICATIONS (COMPUTER EMERGENCY RESPONSE TEAM) REGULATIONS, 2019

ARRANGEMENT OF REGULATIONS

STATUTORY INSTRUMENTS

2019 No. 81.

The Uganda Communications (Computer Emergency Response Team) Regulations, 2019

(Under section 5 (1) (k) and 93 of the Uganda Communications Act, 2013, Act No. 1 of 2013)

IN EXERCISE of the powers conferred upon the Minister by section 93 of the Uganda Communications Act, 2013 and in consultation with the Uganda Communications Commission, these Regulations are made this 5th day of July, 2019.

PART I—PRELIMINARY

1. Title.

These Regulations may be cited as the Uganda Communications (Computer Emergency Response Team) Regulations, 2019.

2. Application.

These Regulations apply to all operators—

(a) for the daily operations of the Computer Emergency Response Team ("CERT"), with or without a communications emergency; and

(b) in the event of a communications emergency declared by the Uganda Communications Commission.

3. Objective of Regulations.

The objective of these Regulations is—

(a) to establish and operate a CERT to manage cyber security incidents in the communications sector;

(b) to identify and protect critical communications infrastructure;

(c) to provide for an administrative and legal framework during a declared communications emergency;

(d) to provide for emergency response measures to respond to cyber and any other network threats in the communications sector.

4. Interpretation.

In these Regulations, unless the context otherwise requires—

"Act" means the Uganda Communications Act, 2013;

"authorised" in relation to an officer or employee of the Commission, means a person authorised by the Executive Director to exercise the powers or perform the duties in respect of which an authorised person is required to perform;

"CERT" means Computer Emergency Response Team;

"communications emergency" means an emergency in the communications subsector declared by the Commission;

"Commission" means the Uganda Communications Commission established by the Act;

"communications" means telecommunications, data communications, radio communications, postal communications and broadcasters;

"communications services" means services performed consisting of the dissemination or interchange of audio, visual or data content using postal, radio or telecommunications media or data communication and includes broadcasting;

"critical communications infrastructure" means an element or system of elements of the critical infrastructure in the communications sector and within the field of cyber security;

"currency point" has the value assigned to it in the Schedule to these Regulations;

"Executive Director" means the Executive Director of the Commission;

"inspector" means a person appointed by the Commission under section 49 of the Act;

"Minister" means the Minister responsible for information and communications technology;

"operator" means a person licensed to provide communication or communications services;

"Tribunal" means the Uganda Communications Tribunal established by section 60 of the Act.

PART II—POWERS OF COMMISSION TO DECLARE AND ACT IN A COMMUNICATIONS EMERGENCY

5. Declaration of a communications emergency.

The Commission may declare a communications emergency in the event of a major threat to communications or a significant cyber related event threatening the operation of critical communications infrastructure in the country.

6. Powers of Commission in a communications emergency.

The Commission may, where it declares a communications emergency—

(a) classify threats to communications for appropriate sector response;

(b) inform the public of any identified threats to protect public safety;

(c) monitor communications services in Uganda;

(d) install equipment at facilities owned by operators to monitor and block communications traffic that may disrupt communications and harm public safety;

(e) confiscate any apparatus which is being operated without a licence;

(f) confiscate any apparatus which is being operated contrary to the directives of the Commission;

(g) direct an operator or other person to provide critical information to assist the Commission in its response to a communications emergency or cyber-crime or any other computer related communications incident;

(h) direct an operator to deny service to a consumer or intermediate user of communications services engaging in prohibited or destructive behavior; and

(i) refer, where necessary, complaints to law enforcement agencies for investigation and prosecution.

PART III—ESTABLISHMENT AND OPERATIONS OF COMPUTER EMERGENCY RESPONSE TEAM (CERT)

7. Establishment of CERT.

(1) There is established a Computer Emergency Response Team within the Commission to protect critical communications infrastructure in the country.

(2) The Commission shall develop and issue guidelines for effective operations of the CERT in the communications sector.

(3) The Commission shall ensure compliance with applicable national standards and international standards laid down by international communication agreements to which Uganda is party with respect to the mandate of the CERT.

8. Responsibilities of CERT.

The CERT shall—

(a) design, manage and implement a critical infrastructure protection program to protect Uganda's critical communication assets in the event of an interference, compromise, incapacitation or integrity problem; including acts of cyber war, espionage or cyber terrorism;

(b) develop operational guidelines to manage and respond to communications incidents;

(c) educate stakeholders within the communications sector on risks and vulnerabilities as they emerge from time to time;

(d) develop, maintain and ensure implementation of cyber security procedures and standards by operators;

(e) develop guidelines for dissemination to the public of information on communications emergencies and cyber security incidents;

(f) classify communications and cyber threats;

(g) coordinate with law enforcement agencies and local and international bodies in cybersecurity management;

(h) forecast, take preventive measures, and broadcast alerts on cyber security incidents;

(i) conduct cyber security audits on critical communications infrastructure;

(j) deploy equipment at the premises and on the network infrastructure of operators;

(k) receive, analyse and investigate cyber security incidents, and take appropriate action;

(l) direct an operator to remove or restrict access to any unlawful, illegal or offensive content from a regulated communications medium;

(m) refer, where necessary, complaints to law enforcement agencies for investigation and prosecution; and

(n) carry out any other responsibilities relating to cyber security management as the Commission may prescribe from time to time.

PART IV—RESPONSIBILITIES OF OPERATORS

9. Obligations and reporting requirements of operators.

(1) An operator shall—

(a) maintain a secure environment for the transmission of voice and data communications at all times;

(b) establish and implement a cyber-security policy for information and communications systems approved by the Commission;

(c) provide a safe space for installation of communications monitoring equipment by the Commission and ensure it is not tampered with or bypassed;

(d) implement guidelines issued by the CERT;

(e) notify the Commission of any significant information or computer security threat or incident that comes to their attention during their ordinary course of business;

(f) provide the Commission with quarterly cyber security incident reports, information technology and systems risk assessment reports and any other information requested for by the Commission;

(g) allow inspectors access to records and premises in the course of an investigation of any communications emergency or incident of alleged cybercrime;

(h) regularly update internal operating standards, guidelines or procedures on the advice of the CERT;

(i) establish reliable and up to date mechanisms to filter malicious traffic from incoming or outgoing traffic;

(j) maintain a designated focal point of contact accessible at all hours by the Commission in the event of an emergency; and

(k) promptly disconnect a consumer, user, third party content provider or other person if directed by the Commission.

10. Information and record keeping.

(1) An operator shall maintain the following information for a period of at least six months—

(a) any action taken by the operator under regulation 9;

(b) user logs, traffic and routing data pertaining to any threat or malicious traffic; and

(c) any other information specified by the Commission.

(2) The Commission may retain the information referred to under subregulation (1) if directed by the Tribunal or a court.

11. Commission to issue guidelines on certain matters.

The Commission shall issue guidelines for the purpose of ensuring that—

(a) there is information security and that no information is shared for purposes other than those specified under the Act and these Regulations;

(b) no information is shared or published in a manner that violates the constitutional and statutory rights of the persons or entities whose information is shared; and

(c) no information is kept longer than is necessary to achieve the purposes specified under these Regulations, and that any such information collected from operators is destroyed in a timely manner.

12. Access to information collected.

(1) Only authorised staff of the Commission and inspectors may collect information and records under these Regulations.

(2) An operator shall afford properly identified staff of the Commission and inspectors referred to under subregulation (1), full access to any information, document, article, apparatus or equipment that is the subject of an investigation under these Regulations.

(3) The entry shall be limited to an operator's place of operation, business or place where the information is stopped.

(4) An entry other than one under subregulation (2) shall require a search warrant issued by a Magistrate.

PART V—MISCELLANEOUS

13. Protection from liability

(1) An officer of the Commission or a person acting on the directions of the Commission or of an officer of the Commission is not personally liable for any act or omission done or omitted to be done in good faith in the exercise of functions under these Regulations.

(2) An operator acting on the directions of the Commission shall not be held liable for any action done in compliance with these Regulations.

14. Offences and penalties.

(1) Any person whether, being an officer of the Commission, a public officer, an operator, private individual or entity who publishes, divulges, discloses or makes known in any manner information collected under these Regulations without obtaining the authority of the Commission commits an offence.

(2) A person who commits an offence under subregulation (1) is liable, on conviction, to a fine not exceeding forty-eight currency points or imprisonment not exceeding two years or both.

(3) Where the person or entity convicted of an offence under this regulation is an operator, the Commission may revoke the operator's licence.

SCHEDULE

Regulation 4.

CURRENCY POINT

A currency point is equivalent to twenty thousand shillings.

FRANK TUMWEBAZE,
Minister of Information and Communications Technology and National Guidance.