STATUTORY INSTRUMENTS
SUPPLEMENT No. 30 8th 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.

S T A T U T O R Y I N S T R U M E N T S

2019 No. 90

THE UGANDA COMMUNICATIONS (CENTRALISED EQUIPMENT IDENTIFICATION REGISTER) REGULATIONS, 2019

ARRANGEMENT OF REGULATIONS

2019 No. 90

The Uganda Communications (Centralised Equipment Identification Register) Regulations, 2019

(Under sections 5 (1) (k), 6 (2) and 93 of the Uganda Communications Commission Act, 2013, Act 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 (Centralised Equipment Identification Register) Regulations, 2019.

2. Application.

These Regulations apply to the Centralised Equipment Identification Registry established under these Regulations to detect and deny communications services operated on unauthorised or blacklisted communications apparatus.

3. Objectives.

The objectives of these Regulations are—

(a) to provide for the operation of the Centralised Equipment Identification Register,

(b) to promote and safeguard the interests of consumers; and

(c) to provide a procedure for reporting the use of unauthorised communications apparatus and a means to disable the functioning of unauthorised, stolen or blacklisted communications apparatus.

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 an officer authorised by the Executive Director to exercise the powers of the Commission or to perform duties in respect of which an authorised person is required;

"black list" means the list of IMEI or ESN entries that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use;

"CEIR" means the Centralised Equipment Identification Register established under regulation 6;

"CEIR Manager" means a person with the necessary technical expertise appointed by an operator with the approval of the Commission, to maintain the CEIR;

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

"counterfeit product" means a product bearing a mark that is identical with or substantially indistinguishable from a genuine registered trademark;

"counterfeit communications apparatus" means—

(a) communications apparatus with an illegitimate IMEI (International Mobile Equipment Identity) or ESN (Electronic Serial Number);

(b) communications apparatus with a cloned IMEI; or

(c) any other communications apparatus with a blank, invalid or incorrect IMEI;

"centralised equipment identity register" means a shared electronic database which holds unique pairs of communications apparatus numbers and IMEIs or ESNs in form of three lists, namely; the white list, grey list and black list;

"Electronic Serial Number" or ESN means a unique code or number used by an electronic communications network to identify individual electronic communications equipment;

"grey list" means the list of IMEI or ESN entries that are temporarily permitted for use on networks;

"GSMA" means Global System for Mobile Association;

"International Mobile Equipment Identification" or IMEI means a unique code used to identify individual mobile equipment communications apparatus in Global Systems for Mobile communications networks;

"operator" means a person or entity licensed by the Commission to provide telecommunications services;

"prohibited communications apparatus" means illegitimate or cloned apparatus without an International Mobile Equipment Identification ("IMEI");

"subscriber" means a consumer of communications services;

"unauthorised communications apparatus" means stolen, counterfeit or other apparatus prohibited by the Commission;

"white list" means the list of IMEI or ESN entries that are permitted for use on the network.

PART II— CENTRALISED EQUIPMENT IDENTIFICATION REGISTER

5. **Functions of Commission.**

(1) The Commission shall —

(a) protect the interests and safety of consumers by directing denial of service to prohibited communications apparatus;

(b) protect the integrity of the communications sector by prohibiting the use of unauthorised apparatus; whether by operators, consumers or other persons;

(c) issue guidelines for the disposal of damaged, blacklisted or obsolete consumer communications apparatus; and

(d) receive and arbitrate consumer complaints with respect to actions taken by operators under these Regulations.

(2) The Commission shall ensure that the CEIR maintains the database of IMEIs and ESNs of all devices registered on the communications networks.

6. Establishment of CEIR and operator obligations.

(1) There is established a Centralised Equipment Identification Register which shall be operated by the Commission.

(2) Every operator shall connect all the network elements to the CEIR; including any new equipment.

(3) Every operator shall declare to the Commission all equipment and network technologies necessary for connection to the CEIR and shall —

(a) ensure that the black, grey and white CEIR lists are kept up—to—date at all times;
(b) ensure that all IMEI or ESN entries are maintained;
(c) take prompt action on any directive of the Commission; and
(d) submit all information requested by the Commission in the requested type, format and frequency.

(4) Every operator shall ensure that their mobile network interfaces are interoperable with the CEIR.

(5) Every operator shall ensure that CEIR equipment does not interfere with any other equipment directed to be installed at the premises of the operator; including the INMS.

7. Functions of Commission in relation to CEIR.

(1) The Commission shall monitor, inspect and oversee the operations of the CEIR by—

(a) providing conducive space and environment to accommodate the CEIR;

(b) providing reliable power to run the CEIR and ensuring that power back up systems are in place;

(c) providing operators with security and access controls to the CEIR equipment;

(d) implementing sanctions against any person found in violation of these Regulations;

(e) arbitrating and determining disputes between operators using the CEIR; and

(f) approving the location where the CEIR is housed.

(2) The CEIR shall remain the property of the operators.

(3) Every operator shall appoint a liaison officer to communicate with the CEIR Manager in the operation of the CEIR.

8. Appointment of CEIR Manager.

(1) The Commission shall appoint a CEIR Manager to maintain the CEIR.

(2) The CEIR Manager shall—

(a) manage the CEIR in accordance with guidelines issued by the Commission from time to time; and

(b) report and cooperate with the police and other law enforcement agencies in all instances where the Manager takes action in accordance with guidelines issued under paragraph (a).

(3) The CEIR Manager shall ensure that the CEIR is able to identify IMEIs including—

(a) IMEIs which are not allocated; and

(b) IMEIs, which are null, duplicate, cloned or zero.

(4) The CEIR data shall contain the following information relating to devices registered with all mobile networks in Uganda—

(a) IMEIs;

(b) IMEI status (white, grey or black list) and the reason for listing;
(c) date of record creation;
(d) date of last record update; and
(e) the device model number.

(5) The CEIR Manager shall ensure that—
(a) the CEIR is able to block services to subscribers with registered devices with invalid or blacklisted IMEIs;
(b) the CEIR is able to identify the device model, version and other information of all the communications devices connected to the network of each operator;
(c) the CEIR is able to allow the creation of a new record in the database containing the IMEIs whenever a new subscriber account is activated;
(d) the CEIR is updated periodically and that the IMEI database is updated with the latest information on valid IMEI assignments by the most efficient method available; and
(e) the CEIR has a facility to access GSMA's IMEI database and has the capacity to identify counterfeit IMEIs of devices connected to communications networks.

(6) The CEIR Manager shall regularly publish the updated local black, white and grey list database information of every operator in order to prevent cloning across networks and to keep the database information up to date.

(7) The database shall support a flexible method of input comprising of a database supported by GSMA and any other method approved by the Commission.

(8) The CEIR Manager shall perform a check on the IMEI format to verify if it is of a valid format and range.

9. Connection to CEIR by operators.

(1) An operator shall connect to the CEIR using the appropriate secured protocol and facilities.

(2) The interfaces supported by the CEIR shall include the standard MAP interface, classic SS7, High Speed SS7, M3UA Sigtran and Diameter for the S13 interface and other interfaces as the Commission may determine.

10. Access to equipment and elements connected to CEIR.

(1) The CEIR manager shall have full access to the CEIR and its operations.

(2) Operators shall have access to the CEIR for data read only.

(3) All operators connecting to the CEIR may only access the CEIR equipment through a person designated by an authorised employee, and through a web based Graphical User Interface (GUI).

(4) Access to the CEIR shall be limited through a password and username provided by the CEIR manager.

(5) Any visitor to a facility where CEIR equipment is housed shall require clearance from the Commission.

(6) The Commission may deny or provide access to the CEIR system.

PART III — PROCEDURE FOR DENYING ACCESS TO NETWORK SERVICES

11. Denial of service to IMEI communications apparatus management.

(1) Where the CEIR detects mobile communications apparatus with an invalid, incorrect or illegitimate IMEI, the CEIR Manager shall take the following action—

(a) move the communications apparatus to the grey list;
(b) using the SMS Alert feature or other viable method, notify the subscriber about the status of their communications apparatus and specify a time frame within which the communications apparatus will be denied service; and
(c) after the expiry of the time frame specified in paragraph (b), move the communications apparatus to the black list and deny access to all services except emergency services.

(2) The time frame referred to in subregulation (1) (b) shall be determined by the Commission in consultation with the operators.

12. Cloned IMEI communications apparatus management.

(1) Where two or more communications devices have the same IMEI, the CEIR Manager shall grey list the devices and allow temporary bypass to the barring function until the device is verified and confirmed as genuine.

(2) The operator shall notify a subscriber by SMS alert of the status of their communications apparatus, and prescribe a time frame within which the subscriber shall be denied service until the subscriber produces for verification, a communications device with a valid IMEI.

13. Management of roaming subscribers.

Where the CEIR detects a roaming subscriber with a manipulated or illegitimate IMEI or cloned IMEI, the CEIR Manager shall take the following action—

(a) using the SMS alert feature, notify the roaming subscriber that their communications apparatus is counterfeit and not acceptable in Uganda;
(b) advise the roaming subscriber to purchase new communications apparatus within 7 days or incur new tariffs for all services; and

(c) after 7 days' notice, apply new tariffs to the roaming subscriber until the subscriber purchases new genuine communications apparatus or leaves the country.

14. Blacklisting of communications apparatus.

(1) The CEIR Manager shall upon receipt of a police statement immediately blacklist all communications apparatus reported as stolen, damaged or lost.

(2) An operator shall deny service to a device blacklisted under subregulation (1).

15. Reporting procedure.

The reporting procedure by a subscriber for failure to access network services shall be as follows—

(a) the subscriber shall call the operator to verify their communications apparatus or return the communications apparatus to the point of purchase;

(b) the intervention of a genuine subscriber with proof of ownership will trigger denial of service to any other device with the same IMEI on expiry of the time prescribed in regulation 12 (2); and

(c) where there is no genuine claim of ownership of the IMEI, all the IMEI pairs will remain on the grey list with temporary bypass to the barring function until genuine ownership is determined.

16. Operator to report to Commission.

(1) Every operator shall report to the Commission on a monthly basis for the first six months, and thereafter on a quarterly basis, the following—

(a) the number of counterfeit communications apparatus denied service;

(b) the trends of counterfeit devices on the network; and

(c) the trends of customer complaints specific to denial of service.

(2) The reporting procedure for stolen, damaged and lost communications apparatus shall be as follows—

(a) a subscriber whose mobile communications apparatus is lost or stolen shall report the loss or theft to the police and make a statement; and shall notify the relevant network service licensee to block the SIM card and communications apparatus from any further use;

(b) where a lost mobile phone is recovered, it shall be reported to the police and the police shall issue a statement or written proof to a person reporting the recovered phone;

(c) the police shall notify the CEIR Manager for white listing of the communications apparatus recovered under paragraph (b);

(d) a subscriber whose mobile phone has been damaged beyond repair shall report the damage to the police for disposal procedures.

(3) Disposal of a communications device shall be done in accordance with the National Environment Act, 2019 and regulations made under that Act.

17. No charges for reporting lost, stolen or damaged equipment.

An operator shall not charge its subscribers or consumers for reporting stolen, damaged or lost mobile communications apparatus.

18. Indemnification of operators.

An operator acting on the directions of the Commission or an authorised officer shall not be liable for any act or omission done in good faith in the exercise of functions under these Regulations.

PART IV — MISCELLANEOUS

19. Confidentiality.

(1) Every operator shall maintain utmost confidentiality of subscriber information and any disclosure of subscriber information to a third party shall be only as authorised by a court order.

(2) The Commission shall ensure that at all times; an operator can only access its own network and only access information specific to that particular operator.

20. Non-discrimination and impartiality.

(1) Any action taken in relation to counterfeit communications apparatus shall be done with fairness and impartiality and in line with the operation guidelines and these Regulations.

(2) It is the responsibility of every operator to ensure that reasons for black listing of communications apparatus are valid and in accordance with the prescribed procedures.

(3) An operator shall effect the blocking of the reported mobile communications apparatus within twenty four hours of its being reported for blacklisting.

21. Offences.

(1) A person who discloses subscriber information to a third party without a court order commits an offence and is liable, on conviction, to a fine not exceeding forty eight currency points or imprisonment not exceeding twenty four months, or both.

(2) The Commission may suspend or revoke the licence of an operator who contravenes these Regulations.

Cross References

The National Environment Act, 2019, Act 5 of 2019

Frank Tumwebaze
Minister of Information, Communications Technology and National Guidance