Amended vide Telecommunications (telecom Cyber Security) Amendment Rules 2025

MINISTRY OF COMMUNICATIONS

(Department of Telecommunications)

NOTIFICATION

New Delhi, the 21st November, 2024.

G.S.R. 720(E).—Whereas a draft of the Telecommunications (Telecom Cyber Security) Rules, 2024, which the Central Government proposes to make in exercise of the powers conferred by sub-section (1) of section 22 read with clause (v) to sub-section (2) of section 56 of the Telecommunications Act, 2023 (44 of 2023), was published as required by sub-section (1) of section 56 of the said Act *vide* notification of the Government of India in the Ministry of Communication, Department of Telecommunication number G.S.R. 520(E), dated the 28th August, 2024, in the Gazette of India, Extraordinary, Part II, section 3, sub-section (i), dated the 28th August, 2024, inviting objections and suggestions from the persons likely to be affected thereby, before the expiry of the period of thirty days from the date on which the copies of the Official Gazette containing the said notification were made available to the public;

And whereas copies of the said Official Gazette were made available to the public on the 29th August, 2024;

And whereas the objections and suggestions received from the public in respect of the said draft rules have been duly considered by the Central Government;

Now, therefore, in exercise of the powers conferred by sub-section (1) of section 22 read with clause (v) to sub-section (2) of section 56 of the Telecommunications Act, 2023 (44 of 2023), and in supersession of the prevention of tampering of the Mobile Device Equipment Identification Number Rules, 2017, except as respects things done or omitted to be done before such supersession and without overriding the terms and conditions of actions taken under those rules, including registrations undertaken in pursuance thereof, the Central Government hereby makes the following rules, namely:-

1. Short title and commencement. — (1) These rules may be called the Telecommunications (Telecom Cyber Security) Rules, 2024.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions. — (1) In these rules, unless the context otherwise requires,–

(a) "Act" means the Telecommunications Act, 2023 (44 of 2023);

(b) "certified agency" means the agency specified by the Central Government on the portal to carry out security audit;

(c) "Chief Telecommunication Security Officer" means the designated employee of a telecommunication entity, appointed under rule 6;

(ca) ―licensee‖ means a person holding a license to provide telecommunication services under the Indian Telegraph Act, 1885 (13 of 1885);

(cb) ―MNV platform‖ means the mobile number validation platform established under rule 7A to enable validation by authorised entities and licensees as regards whether telecommunication identifiers specified by TIUE customers or users, correspond to the users as present in the database of an authorised entity or licensee, as the case may be';

(d) "portal" means the portal as notified by the Central Government under sub-rule (1) of rule 10;

(e) "security incident" means an event having real or potential risk on telecom cyber security;

(f) "telecom cyber security" means cyber security of telecommunication networks and telecommunication services which includes tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, assurance and technologies that can be used to safeguard telecommunication networks and telecommunication services against relevant security risks in the cyber environment;

(g) "telecommunication entity" means any person providing telecommunication services, or establishing, operating, maintaining, or expanding telecommunication network, including an authorised entity holding an authorisation under sub-section (1) of section 3 of the Act, or a person exempted from the requirement of authorisation under sub-section (3) of section 3 of the Act; and

(h) "telecommunication equipment identification number" means a telecommunication identifier bearing—

(i) international mobile equipment identity (IMEI) number; or

(ii) electronic serial number (ESN); or

(iii) any other number or signal that identifies a unique telecommunication equipment.

_(i) —TIUE (telecommunication identifier user entity)‖ means a person, other than a licensee or authorised entity, which uses telecommunication identifiers for the identification of its customers or users, or for provisioning, or delivery of services‘.

(2) Words and expressions used in these rules and not defined herein but defined in the Act, shall have the meanings respectively assigned to them in the Act.

3. Collection, sharing and analysis of data. — (1) The Central Government, or any agency authorised by the Central Government, may, for the purposes of protecting and ensuring telecom cyber security, —

~~(a)~~ seek from a telecommunication entity, traffic data and any other data, other than content of messages, in the form and manner as may be specified by the Central Government on the portal; ~~and~~

(aa) seek data related to telecommunication identifiers used by a TIUE in the form and manner as specified on the portal; and

(b) direct a telecommunication entity to establish necessary infrastructure and equipment for collection and provision of such data from designated points to enable its processing and storage.

(2) The data collected under sub-rule (1) may be analysed for taking measures to enhance telecom cyber security, and such analysis may, to the extent determined by the Central Government as necessary for protecting and ensuring telecom cyber security, be—

(a) disseminated to any agency of the Central Government engaged in law enforcement and security related activities; and

(b) shared with telecommunication entities or TIUE or users:

Provided that any data so disseminated or shared, shall not be used for any purpose, other than for ensuring telecom cyber security.

(3) The Central Government and any agency authorised by the Central Government to collect data under these rules, as well as persons with whom such data is shared under sub-rule (2), shall put in place adequate safeguards, including any specific safeguards as may be specified by the Central Government to ensure that such data is stored and maintained in strict confidentiality and prevent any unauthorised access thereto.

4. Obligations relating to telecom cyber security. — (1) No person shall –

(a) endanger telecom cyber security; or

(b) send any message which adversely affects telecom cyber security.

(2) Without prejudice to the generality of sub-rule (1), no person shall endanger telecom cyber security by misuse of telecommunication equipment or telecommunication identifier or telecommunication network or telecommunication services or by –

(a) fraud, cheating or personation;

(b) transmitting any message which is fraudulent;

(c) committing or intending to commit any security incident;

(d) engaging in any other use which is contrary to the provision, of any other law for the time being in force; or

(e) any other means which may have security risk on telecom cyber security.

(3) Every telecommunication entity and TIUE shall ensure compliance with the directions and standards, including timelines for their implementation, as may be issued by the Central Government for the prevention of misuse of telecommunication identifiers or telecommunication equipment or telecommunication network or telecommunication services for ensuring telecom cyber security.

(4) Every telecommunication entity and TIUE shall implement the following measures to ensure telecom cyber security, namely :—

(a) adopt a telecom cyber security policy, which shall include—

(i) security safeguards, risk management approaches, actions, training, best practices and technologies, to enhance telecom cyber security;

(ii) telecommunication network testing including hardening, vulnerability assessment and penetration testing;

(iii) risk assessment, identification and prevention of security incidents;

(iv) rapid action system to deal with security incidents including mitigation measures to limit the impact of such incidents; and

(v) forensic analysis of security incidents to ensure learnings from such incidents and further strengthening telecom cyber security;

(b) inform the Central Government on adoption of the policy referred to in sub-clause (a), in the manner as may be determined by the Central Government;

(c) identify and reduce the risks of security incidents and ensure timely responses to such incidents;

(d) take appropriate action for addressing security incidents, and mitigate their impact;

(e) ensure implementation of directions and standards issued by the Central Government on telecom cyber security;

(f) conduct periodic telecom cyber security audits of its network to assess resilience to threats on telecom cyber security through its own mechanisms and through the certified agency in such intervals as may be specified by the Central Government on the portal, and share the audit report with the Central Government, which may undertake further audits if so required;

(g) report security incidents to the Central Government, or any officer authorised in this behalf by the Central Government, and measures taken to address such incidents in the manner specified in rule 7;

(h) establish facilities such as Security Operations Centre (SOC), by itself or in collaboration with other telecommunication entities, within the time period as may be specified by the Central Government under sub-rule (3), to address the following, namely:

(i) monitor telecom cyber security and security incidents, intrusions and breaches of telecommunication services or telecommunication network, as well as, attempts to cause such incidents, intrusions or breaches;

(ii) maintain details of threat actors impacting its telecommunication services, or telecommunication network;

(iii) maintain command logs of operation and maintenance;

(iv) maintain logs of Security Operations Centre (SOC) (firewall, Intrusion Detection System (IDS) or Intrusion Prevention System (IPS), or Security Information and Event Management (SIEM) or other such solution);

(v) maintain logs of elements of telecommunication service, or telecommunication network or any other element required for security of telecommunication service or telecommunication network;

(vi) maintain all records or logs specified in this sub-rule, for a period as specified on the portal by the Central Government, and make such records available to the person authorised by the Central Government in this behalf; and

(vii) provide necessary support to the person authorised by the Central Government, including law enforcement agencies for the purpose of investigation related to security incidents.

(5) Every telecommunication entity shall furnish a detailed report relating to the action taken by it under sub-rule (4) in the form and manner as may be specified on the portal.

(6) The Central Government may, pursuant to any report or other information received from a telecommunication entity under sub-rule (4), may —

(a) seek further clarifications from such telecommunication entity; or

(b) issue any directions, orders or instructions to such telecommunication entity for the protection of telecom cyber security and mitigate risks to telecom cyber security.

5. Measures to protect and ensure telecom cyber security.—

(1) The Central Government may put in place digital and other mechanisms as it may consider necessary to identify, or for enabling any person to identify and report, acts that may endanger telecom cyber security.

(2) The Central Government shall, after examination of the information received under sub-rule (1), identify the telecommunication identifier, the use of which is alleged to have endangered telecom cyber security and the person to whom such telecommunication identifier has been issued, by the telecommunication entity, and issue a notice to such person, with details thereof.

(3) The person to whom notice is issued under sub-rule (2), shall send a written response to the Central Government within seven days of receipt of such notice, and if no response is received within such period, the Central Government shall proceed to issue an order under sub-rule (5).

(4) If a response is received from the recipient of the notice under sub-rule (2) within the time specified in sub-rule (3), the Central Government shall, after giving such person a reasonable opportunity of being heard, make an order thereon as it thinks fit under sub-rule (5).

(5) The Central Government shall, based on its assessment of facts and submissions, if any, made by the person to whom notice is issued under sub-rule (2), pass an order, with reasons to be recorded in writing, which may include

directions to the telecommunication entity to —

(a) temporarily suspend use of the relevant telecommunication identifier, in the manner and for a duration as may be specified in such order; or

(b) permanently disconnect the use of the relevant telecommunication identifier.

(6) Where the Central Government considers that immediate action under sub-rule (5) is necessary or expedient in the public interest, it shall without issuing a notice under sub-rule (2), pass an order recording the reasons thereof, with appropriate direction—
(a) to the telecommunication entity to temporarily suspend use of the relevant telecommunication identifier; and
(b) to the TIUE to temporarily suspend use of the relevant telecommunication identifier for identification of or for delivery of message or services to its customers or users.‖;

(7) A copy of the order under sub-rule (5) or sub-rule (6), as the case may be, shall be provided to the person referred to in sub-rule (2) or the telecommunication entity and TIUE referred to in sub-rule (6) or such person affected by the order, and such person or, as the case may be, the telecommunication entity, and TIUE may, within a period of thirty days from the date of issuance of the order, represent to the Central Government in writing, with reasons why such action should not be taken.

(8) The Central Government shall, after giving the person to whom copy of the order has been provided under sub-rule (7), a reasonable opportunity of being heard and for reasons to be recorded in writing, pass an order, either upholding, or modifying, or revoking the order passed under sub-rule (5) or sub-rule (6):

—Provided that any modification of the order under sub-rule (6) may also include an order directing:

(a) the telecommunication entity to permanently disconnect the use of the relevant telecommunication identifier as specified under clause (b) of sub-rule (5); and

(b) the TIUE to prohibit or circumscribe the use of relevant telecommunication identifiers for identification of its customers or users, or for delivery of message or services, in the manner as may be specified in such order to enable the reuse of relevant telecommunication identifiers

(9) Any order of suspension or permanent disconnection of use of the relevant telecommunication identifier under sub-rule (5), sub-rule (6) or sub-rule (8) may also be extended to the other telecommunication equipment or telecommunication identifier linked to the person whose telecommunication identifier has been identified under sub-rule (2) or other telecommunication identifier issued to the person identified under sub-rule (2).

(10) The Central Government may maintain a repository of persons and telecommunication identifiers which have been acted upon pursuant to the orders under sub-rule (5), or sub-rule (6), or sub-rule (8), or sub-rule (9), and may direct telecommunication entities, to prohibit or limit the access to telecommunication service to such persons for a period not exceeding three years from the date of such order.

(11) The Central Government may, if it considers necessary, or pursuant to any request made by any person providing services that are linked to telecommunication identifiers, and TIUE share the list of telecommunication identifiers that have been acted upon pursuant to orders under sub-rule (5), or sub-rule (6), or sub-rule (8), or sub-rule (9), with such persons and, by order, direct such persons to also prohibit or circumscribe the use of such telecommunication identifiers for identification of their customers or users or for delivery of services, in the manner as may be specified in such order.

(12) Any telecommunication identifier, which is subject to suspension or permanent disconnection under this rule, shall not be reallocated to any other person for a period of one year from the date of issuance of the order of suspension or permanent disconnection which may be extended upto three years, for reasons to be recorded in writing, in specific cases.

6. Chief Telecommunication Security Officer. — (1) Every telecommunication entity shall appoint a Chief Telecommunication Security Officer, whose details shall be provided in writing to the Central Government in the form as may be specified on the portal and any replacement or change of such officer shall be promptly intimated to the Central Government, in such form as may be specified on the portal by that Government.

(2) The Chief Telecommunication Security Officer shall be a citizen and resident of India, and responsible to the Board of Directors or similar governing body of the telecommunication entity.

(3) The Chief Telecommunication Security Officer shall be responsible for coordinating with the Central Government on behalf of the telecommunication entity for the implementation of these rules, including compliance with any reporting requirements or reporting of security incidents under rule 7.

7. Reporting of security incidents. — (1) The telecommunication entity shall–

(a) within six hours of becoming aware of a security incident affecting its telecommunication network or telecommunication service, report the same to the Central Government with relevant details of the affected system including the description of such incident; and

(b) within twenty-four hours of becoming aware of such incident, furnish the following information, as applicable:

(i) the number of users affected by the security incident;

(ii) the duration of the security incident;

(iii) the geographical area affected by the security incident;

(iv) the extent to which the functioning of the telecommunication network or telecommunication service is affected;

(v) the remedial measures taken or proposed to be taken; and

(vi) any other information it considers relevant.

(2) The Central Government may, where it determines that disclosure of the security incident is in the public interest, inform the public of such security incident, or require the affected telecommunication entity to do so.

(3) The Central Government may require the affected telecommunication entity to —

(a) provide information needed to assess the security of the telecommunication network and telecommunication service including telecom cyber security policy;

(b) carry out a security audit by a certified agency as may be determined by the Central Government.

(4) The Central Government may issue directions including measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and may also specify the time limits for implementation of such directions to the affected telecommunication entity.

7A. Validation of telecommunication identifiers. —

(1) The Central Government, for ensuring telecom cyber security and preventing security incidents, shall either by itself, or through an agency authorised by it, establish a MNV platform and issue directions to authorised entities and licensees to participate on such platform.

(2) The following entities may place a request on the MNV platform and upon payment of fees, as specified therein, seek validation as to whether the telecommunication identifiers as specified by their customers or users, correspond to the users as available in the database of an authorised entity or licensee:—

(a) a TIUE, either suo moto, or upon a direction from Central or State Government or an agency authorised by the Central or State Government; or

(b) the Central Government or State Government or any agency authorised by the Central Government or State Government: Provided that where a TIUE places a request suo moto on the MNV platform, the decision to allow use of such platform shall rest with the Central Government.

(3) The fees charged for use of the MNV platform shall be shared between the Central Government or its agency that has established and maintains the MNV platform and the authorised entity or licensee providing the validation services, as specified on the portal.

(4) The MNV platform shall transmit any request received under sub-rule (2) or sub-rule (3) to authorised entities and licensees for the purpose of validation, and such entities shall undertake such validation and provide their response to the MNV platform, as specified therein.

(5) The mobile number validation under this rule shall facilitate validation of customers or users associated with a telecommunication identifier for the purpose of services linked to such identifier, and the TIUE, authorised entity and licensee, as the case may be, shall ensure compliance with applicable laws relating to data protection for this purpose.‖.

8. Obligations relating to telecommunication identifier and telecommunication equipment.— (1) A manufacturer of equipment that has International Mobile Equipment Identity (IMEI) number, shall register such IMEI number of such equipment manufactured in India with the Central Government, prior to the first sale of such equipment, in the form as may be specified for such purpose on the portal by that Government.

(2) An importer of equipment that has an International Mobile Equipment Identity (IMEI) number, shall register such IMEI number of such equipment imported into India for sale or testing or research or for any other purpose, with the Central Government, prior to the import of such equipment into India, in the form as may be specified for such purpose on the portal.

(3) No person shall —

(a) intentionally remove, obliterate, change, or alter the unique telecommunication equipment identification number; or

(b) intentionally use, produce, traffic in, have control or custody of, or possess hardware or software related to the telecommunication identifier or telecommunication equipment, knowing it has been configured as specified above.

(4) The Central Government may issue directions to manufacturers of telecommunication equipment bearing International Mobile Equipment Identity (IMEI) number to provide assistance as required in relation to tampered telecommunication equipment or IMEI number.

(4A) The Central Government may issue directions to manufacturers of telecommunication equipment bearing International Mobile Equipment Identity (IMEI) number not to assign IMEIs that are already in

use in telecommunication networks in India to new telecommunication equipment that are manufactured in India or imported to India from the date as specified by the Central Government on the portal.‖

(5) The Central Government may issue directions to telecommunication entities to block the use of telecommunication equipment with tampered International Mobile Equipment Identity (IMEI) number in telecommunication networks or telecommunication services.

(6) The Central Government shall, either directly or through an agency authorised by it, maintain a database of IMEIs which are tampered, or whose use has been restricted.

(7) A person engaged in the sale and purchase in India of used telecommunication equipment bearing IMEI numbers or its authorised agency shall, prior to such sale or purchase access the database specified in sub-rule (6) on payment of fees as specified on the portal and ensure that it shall not directly or indirectly undertake sale or purchase of any telecommunication equipment bearing IMEI number that is specified in such database.

(8) Every manufacturer or importer of any telecommunication equipment that bears an International Mobile Equipment Identity (IMEI) number shall ensure compliance with the directions as may be issued by the Central Government for the purpose of giving effect to these rules.

9. Contravention of rules. — Save as otherwise provided, any contravention of the provisions of these rules shall be dealt with in accordance with the provisions of the Act.

10. Digital Implementation. — (1) The Central Government shall, notify a portal for the purpose of digital implementation of these rules and may also specify any other implementing mechanism.

(2) Where the Central Government considers it necessary to use any secure mode of communication, other than through the portal, for the issuance of any orders, directions or instructions to telecommunication entities and TIUEs or manufacturers or importers of telecommunication equipment, or for collection of any information from such telecommunication entities, and TIUEs , it may use such secure mode of communication.

(3) Every telecommunication entity and TIUEs and manufacturer or importer of telecommunication equipment shall ensure compliance with the obligations relating to reporting or submission of information to the Central Government under these rules using the portal or through a secure mode of communication as may be determined by the Central Government.

[F. No. 24-07/2024-UBB]

DEVENDRA KUMAR RAI, Jt. Secy.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.