

Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024¹

Whereas a draft of the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, which the Central Government proposes to make in exercise of the powers conferred by sub-section (4) of section 22 read with clause (w) of 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 Communications, Department of Telecommunications number G.S.R. 521(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 (4) of section 22 read with clause (w) of sub-section (2) of section 56 of the Telecommunications Act, 2023 (44 of 2023), the Central Government hereby makes the following rules, namely:-

1. Short title and commencement. – (1) These rules may be called the Telecommunications (Critical Telecommunication Infrastructure) 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) “Chief Telecommunication Security Officer” means the Chief Telecommunication Security Officer appointed under rule 6 of the Telecommunications (Telecom Cyber Security) Rules, 2024;
- (c) “Critical Telecommunication Infrastructure” means any telecommunication network, or part thereof, notified under sub-section (3) of section 22 of the Act;
- (d) “portal” means the portal notified by the Central Government under sub-rule(1) of rule 10;

¹ Vide G.S.R. 723(E), dated 22.11.2024, published in the Gazette of India, Extra., Pt. II, Sec. 3(i), dated 22.11.2024.

- (e) “security incident” shall have the same meaning assigned to it in clause (f) of sub-rule (1) of rule 2 of the Telecommunications (Telecom Cyber Security) Rules, 2024; and
- (f) “telecommunication entity” shall have the same meaning assigned to it in clause (g) of sub-rule (1) of rule 2 of the Telecommunications (Telecom Cyber Security) Rules, 2024.

(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. Application. – (1) These rules shall apply to telecommunication network, or any part thereof, which has been notified by the Central Government as Critical Telecommunication Infrastructure under sub-section (3) of section 22 of the Act, based on an assessment that disruption of such infrastructure shall have a debilitating impact on national security, economy, public health or safety of the nation.

(2) The Central Government shall specify on the portal the form and manner in which every telecommunication entity shall provide the details of its telecommunication network, telecommunication services, and elements of such network and services.

4. Compliance requirements. - Every telecommunication entity shall ensure that Critical Telecommunication Infrastructure, including any spares, hardware and software used in such Critical Telecommunication Infrastructure, are in compliance with the following standards, namely:–

- (a) Essential Requirements (ERs), Interface Requirements (IRs), Indian Telecommunication Security Assurance Requirements (ITSARs) and specifications, testing requirements, or conformity assessment, as applicable, issued by Telecommunication Engineering Centre, National Centre for Communication Security, or any other person as may be notified by the Central Government for this purpose:

Provided that in the absence of such standards, a telecommunication entity may utilise only such Critical Telecommunication Infrastructure, including any spares, hardware and software used in such Critical Telecommunication Infrastructure, which meet the relevant standards as may be notified by the Central Government in this regard;

- (b) National Security Directive on Telecommunication Sector (NSDTS) as issued by the Central Government;

- (c) directives on communication security certification issued by the Central Government; and
- (d) such other standards applicable to Critical Telecommunication Infrastructure, as may be notified by the Central Government from time to time.

5. Inspection of Critical Telecommunication Infrastructure. – (1) The Central Government, may, by an order, authorise its personnel to access and inspect hardware, software and data pertaining to Critical Telecommunication Infrastructure of telecommunication entities.

(2) Every telecommunication entity shall ensure access to any personnel authorised by the Central Government under sub-rule (1) for inspection of Critical Telecommunication Infrastructure.

6. Chief Telecommunication Security Officer. – (1) The Chief Telecom Security Officer shall be responsible for the implementation of these rules.

(2) The Central Government shall specify on the portal, the form and manner in which every telecommunication entity shall provide the details in respect of Critical Telecommunication Infrastructure, including the following details, namely:–

- (a) telecommunication network architecture of the Critical Telecommunication Infrastructure;
- (b) authorised personnel having access to Critical Telecommunication Infrastructure;
- (c) inventory of hardware, software and spares related to Critical Telecommunication Infrastructure;
- (d) details of vulnerability, threat or risk analysis for the cyber security architecture of Critical Telecommunication Infrastructure;
- (e) Cyber Crisis Management Plan for Critical Telecommunication Infrastructure;
- (f) security audit reports and audit compliance reports of Critical Telecommunication Infrastructure;
- (g) Service Level Agreements (SLAs) of services pertaining to Critical Telecommunication Infrastructure;
- (h) all logs relating to Critical Telecommunication Infrastructure to assist in detection of anomalies and enable the Central Government to generate intelligence on real time basis; and
- (i) reporting of security incidents within the timelines specified for Critical Telecommunication Infrastructure under rule 7.

7. Obligations related to Critical Telecommunication Infrastructure. – (1) Every telecommunication entity shall comply with the following obligations, namely:–

- (a) ensure security of Critical Telecommunication Infrastructure, including through compliance with the standards as provided under rule 4;
- (b) maintain a complete list of Critical Telecommunication Infrastructure along with the software and hardware details, as well as the dependencies on such Critical Telecommunication Infrastructure;
- (c) preserve in a secure manner, for a minimum period of two years or such other period as may be determined by the Central Government, logs and documentation of the telecommunication network architecture of Critical Telecommunication Infrastructure, including changes in such telecommunication network architecture;
- (d) plan, develop and maintain adequate verification practices and protocols applicable for all personnel authorised to have access to Critical Telecommunication Infrastructure, and undertake periodic review of the same as directed by the Central Government;
- (e) maintain records of the supply chain of the telecommunication equipment and other equipment deployed in the Critical Telecommunication Infrastructure till such infrastructure is in use, and provide such records, as and when sought for by the Central Government;
- (f) ensure that vulnerability or threat or risk analysis for telecommunication network architecture of Critical Telecommunication Infrastructure is carried out annually or in such intervals as may be directed by the Central Government ;
- (g) plan, develop, maintain and review processes required for Service Level Agreements (SLAs) entered into by the telecommunication entities with their vendors in relation to Critical Telecommunication Infrastructure;
- (h) plan, develop, maintain and review processes of taking regular backup of logs of networking and communication devices, servers, systems and services supporting the functioning of the Critical Telecommunication Infrastructure;
- (i) implement standard operating procedures for security incident response systems, including disaster recovery and business continuity;
- (j) implement mechanisms to ensure intimation of security incident(s) to the Central Government, no later than six hours of occurrence of such incident, in the form and manner as may be specified on the portal; and
- (k) maintain a risk register including a graded risk assessment associated with different elements of Critical Telecommunication Infrastructure within its network, identifying

the potential and severity of risks posed to the Critical Telecommunication Infrastructure and solutions to mitigate the same and produce such information as and when sought for by the Central Government.

(2) Where a telecommunication entity requires remote access to its Critical Telecommunication Infrastructure for the purpose of repair or maintenance from a location outside of the territory of India, it shall do so only from such location for which it has obtained prior written approval from the Central Government, and it shall, for each instance of such remote access –

- (a) provide due intimation of such remote access to the Central Government in the form and manner specified on the portal; and
- (b) ensure that the logs for such remote access are preserved for at least one year and provided as and when sought for by the Central Government.

(3) Every telecommunication entity shall furnish a detailed report relating to the action taken by it under sub-rule (1) in the form and manner as may be specified on the portal.

(4) The Central Government may, pursuant to any report or other information received from a telecommunication entity under sub-rule (3),—

- (a) seek further clarifications from such telecommunication entity; or
- (b) issue any directions, orders or instructions to such telecommunication entity for the protection of Critical Telecommunication Infrastructure or mitigating risks to such infrastructure.

8. Requirements for upgradation of Critical Telecommunication Infrastructure. – (1) Where upgradation of the software or hardware of equipment which form part of the Critical Telecommunication Infrastructure is required, the telecommunication entity shall make an application to the Central Government, along with details of the test reports for such upgradation and other relevant information in the form and manner as may be specified on the portal by that Government.

(2) The Central Government shall, within fourteen days of receipt of the application under sub-rule (1),—

- (a) seek any further clarifications if required from the telecommunication entity;
- (b) issue directions to such entity to conduct further testing under sub-rule (3); or
- (c) approve or reject the application for upgradation activity.

(3) The Central Government may direct a telecommunication entity to test any upgradation in the Critical Telecommunication Infrastructure in an appropriate controlled environment and submit the results of such tests in the form and manner, as may be specified by the Central

Government on case to case basis, and the telecommunication entity shall comply with such directions.

(4) Where the Central Government does not seek any clarification or issue directions or specify its approval or rejection under sub-rule (2) within a period of fourteen days from the date of receipt of such application, the telecommunication entity may proceed with such upgradation activity:

Provided that where the Central Government has sought clarifications under sub-rule (2), such time period of fourteen days shall be considered from the date of submission of clarification by such telecommunication entity:

Provided further that where the Central Government has directed to test the upgradation under sub-rule (3), such time period of fourteen days shall be considered from the date of submission of the results of such tests in the form and manner as may be specified by the Central Government on case to case basis through secure mode.

(5) Where upgradation is necessary for addressing or mitigating the adverse effects of a security incident, a telecommunication entity may undertake immediate upgradation in the software or hardware of any equipment that forms part of Critical Telecommunication Infrastructure without making an application under sub rule (1) and within twenty-four hours of such upgradation, report to the Central Government in the form and manner as may be determined by the Central Government, with relevant details of –

(a) the description of the concerned security incident; and

(b) the relevant software or hardware of an equipment requiring upgradation and the nature of upgradation undertaken in respect of such equipment.

(6) The Central Government may, upon receipt of information under sub-rule (5), seek further information or clarifications from the telecommunication entity, or issue directions for further testing and reporting, as it may consider necessary.

(7) The telecommunication entity shall ensure preservation of records and information in relation to any upgradation, till such time the relevant Critical Telecommunication Infrastructure is in use, and such records shall be produced as and when sought by the Central Government.

(8) Nothing in this rule shall apply to a routine software update aimed to incrementally improve performance or security of Critical Telecom Infrastructure.

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, or for collection of any information from such telecommunication entities, it may use such secure mode of communication on case to case basis.

(3) Every telecommunication entity 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 determined by the Central Government.

[No.24-08/2024-UBB]

Devendra Kumar Rai,
Joint Secretary to the Government of India.