रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-29082024-256725
CG-DL-E-29082024-256725

असाधारण
EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (i)
PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 482] नई दिल्ली, बुधवार, अगस्त 28, 2024/ भाद्र 6, 1946
No. 482] NEW DELHI, WEDNESDAY, AUGUST 28, 2024/ BHADRA 6, 1946

संचार मंत्रालय

(दूरसंचार विभाग)

अधिसूचना

नई दिल्ली, 28 अगस्त, 2024

सा.का.नि. 521(अ.).—निम्नलिखित प्रारूप नियम जिसे केंद्रीय सरकार दूरसंचार अधिनियम, 2023 (2023 का 44) की धारा 56 की उप-धारा (2) के खंड (ब) के साथ पठित धारा 22 की उप-धारा (4) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए बनाने का प्रस्ताव करती है, को इससे प्रभावित होने वाले सभी व्यक्तियों की सूचना के लिए एतद्वारा प्रकाशित किया जाता है और एतद्वारा नोटिस दिया जाता है कि उक्त प्रारूप नियम पर उस तारीख से तीस दिन की अवधि की समाप्ति के पश्चात विचार किया जाएगा जिस तारिख से सरकारी राजपत्र में यथा प्रकाशित इस अधिसूचना की प्रतियां सर्वसाधारण को उपलब्ध कराई जाती हैं;

यदि कोई, आपत्ति अथवा सुझाव हो, तो उसे संयुक्त सचिव (दूरसंचार), दूरसंचार विभाग, संचार मंत्रालय, भारत सरकार, संचार भवन, 20, अशोक रोड, नई दिल्ली-110001 को भेजा जा सकता है;

केंद्रीय सरकार द्वारा उक्त अवधि की समाप्ति से पूर्व उक्त प्रारूप नियम के संबंध में किसी भी व्यक्ति से प्राप्त आपत्ति अथवा सुझाव पर विचार किया जाएगा।

1. संक्षिप्त नाम और प्रारंभ

(1) इन नियमों को दूरसंचार (महत्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024 कहा जाएगा।

(2) ये सरकारी राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे।

2. परिभाषाएं

(1) इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो:

(क) **"अधिनियम"** से दूरसंचार अधिनियम, 2023 (2023 का 44) अभिप्रेत है;

(ख) **"मुख्य दूरसंचार सुरक्षा अधिकारी"** से दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 के अनुसरण में नियुक्त दूरसंचार कंपनी का नामोद्दिष्ट कर्मचारी अभिप्रेत है;

(ग) **"महत्वपूर्ण दूरसंचार अवसंरचना"** से अधिनियम की धारा 22 की उप-धारा (3) के अंतर्गत अधिसूचित कोई भी दूरसंचार नेटवर्क अथवा उसका कोई भाग अभिप्रेत है;

(घ) **"नियम"** से दूरसंचार (महत्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024 अभिप्रेत है;

(ङ) **"सुरक्षा घटना"** से दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 के अंतर्गत दिया गया अर्थ अभिप्रेत है; और

(च) **"दूरसंचार कंपनी"** से तात्पर्य किसी ऐसे व्यक्ति से है जो दूरसंचार सेवाएं प्रदान करता है अथवा दूरसंचार नेटवर्क की स्थापना, प्रचालन, अनुरक्षण अथवा विस्तार करता है जिसमें अधिनियम की धारा 3 की उप-धारा (1) के अंतर्गत प्राधिकार रखने वाली प्राधिकृत इकाई अथवा अधिनियम की धारा 3 की उप-धारा (3) के अंतर्गत प्राधिकार की आवश्यकता से छूट प्राप्त व्यक्ति शामिल हैं;

(2) उन शब्दों और पदों जिनका उपयोग इन नियमों में किया गया है और जिन्हें परिभाषित नहीं किया गया है परन्तु जिन्हें अधिनियम में परिभाषित किया गया है, के वही अर्थ होगें जो अधिनियम में विनिर्दिष्ट किया गया है।

3. अनुप्रयोज्यता

(1) ये नियम दूरसंचार नेटवर्क अथवा उसके किसी भाग पर लागू होंगे जिसे केन्द्रीय सरकार द्वारा अधिनियम की धारा 22 की उप-धारा (3) के प्रावधानों के अनुसार महत्वपूर्ण दूरसंचार अवसंरचना के रूप में अधिसूचित किया गया है, जो इस आकलन पर आधारित है कि ऐसी अवसंरचना के विघटन से राष्ट्रीय सुरक्षा, अर्थव्यवस्था, सार्वजनिक स्वास्थ्य अथवा राष्ट्र की सुरक्षा पर प्रतिकूल प्रभाव पड़ेगा।

(2) महत्वपूर्ण दूरसंचार अवसंरचना की अधिसूचना को सक्षम बनाने के लिए प्रत्येक दूरसंचार कंपनी अपने दूरसंचार नेटवर्क, दूरसंचार सेवाओं, ऐसे नेटवर्क और सेवाओं के घटकों तथा सॉफ़्टवेयर तथा हार्डवेयर सहित अन्य संगत सूचना का विवरण, केन्द्रीय सरकार के अनुरोध पर, इस प्रयोजन के लिए निर्दिष्ट प्रपत्र में प्रदान करेगी।

4. अनुपालन आवश्यकताएँ

(1) दूरसंचार कंपनी यह सुनिश्चित करेगी कि महत्वपूर्ण दूरसंचार अवसंरचना जिसमें ऐसी महत्वपूर्ण दूरसंचार अवसंरचना में उपयोग किया जाने वाला कोई भी पुर्जा, हार्डवेयर और सॉफ़्टवेयर शामिल हैं, निम्नलिखित का अनुपालन कर रहे हैं:

(क) अनिवार्य आवश्यकताएँ (ईआर), इंटरफ़ेस आवश्यकताएँ (आईआर), भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (आईटीएसएआर) और दूरसंचार अभियांत्रिकी केंद्र, राष्ट्रीय संचार सुरक्षा केंद्र अथवा किसी अन्य व्यक्ति द्वारा जारी विनिर्देशों, परीक्षण आवश्यकताओं अथवा अनुरूपता मूल्यांकन जिसे इस उद्देश्य के लिए केंद्रीय सरकार द्वारा अधिसूचित किया जाएगा;

(ख) केंद्रीय सरकार द्वारा जारी और समय-समय पर यथासंशोधित दूरसंचार क्षेत्र संबंधी राष्ट्रीय सुरक्षा निदेश (एनएसडीटीएस); और

(ग) केंद्रीय सरकार द्वारा जारी संचार सुरक्षा प्रमाणन संबंधी दिशा-निर्देश।

(2) दूरसंचार कंपनी महत्वपूर्ण दूरसंचार अवसंरचना संबंधी मानकों का अनुपालन सुनिश्चित करेगी जिन्हें समय-समय पर केंद्रीय सरकार द्वारा अधिसूचित अथवा निर्धारित किया जाएगा।

5. महत्वपूर्ण दूरसंचार अवसंरचना का निरीक्षण

(1) केंद्रीय सरकार, आदेश द्वारा, अपने कार्मिकों को दूरसंचार कंपनियों की महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित हार्डवेयर, सॉफ़्टवेयर और डेटा को एक्सेस करने और उसका निरीक्षण करने के लिए प्राधिकृत कर सकती है ।

(2) दूरसंचार कंपनी महत्वपूर्ण दूरसंचार अवसंरचना के निरीक्षण के लिए उप-नियम (1) के अंतर्गत केंद्रीय सरकार द्वारा प्राधिकृत किसी भी कार्मिक को एक्सेस सुनिश्चित करेगी।

6. मुख्य दूरसंचार सुरक्षा अधिकारी

मुख्य दूरसंचार सुरक्षा अधिकारी इन नियमों के कार्यान्वयन हेतु उत्तरदायी होगा और वह केन्द्रीय सरकार को निर्दिष्ट प्रपत्र और तरीके से महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित निम्नलिखित विवरण उपलब्ध कराएगा:

(क) महत्वपूर्ण दूरसंचार अवसंरचना का दूरसंचार नेटवर्क आर्किटेक्चर;

(ख) महत्वपूर्ण दूरसंचार अवसंरचना तक पहुंच रखने वाले प्राधिकृत कार्मिक;

(ग) महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित पुर्जों, हार्डवेयर और सॉफ्टवेयर की सूची;

(घ) महत्वपूर्ण दूरसंचार अवसंरचना की साइबर सुरक्षा आर्किटेक्चर के लिए भेद्यता/खतरा/जोखिम विश्लेषण का विवरण;

(ङ) महत्वपूर्ण दूरसंचार अवसंरचना के लिए साइबर संकट प्रबंधन योजना

(च) महत्वपूर्ण दूरसंचार अवसंरचना की सुरक्षा लेखापरीक्षा रिपोर्ट और लेखापरीक्षा की अनुपालन रिपोर्ट; और

(छ) महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित सेवाओं का सेवा स्तर करार (एसएलए);

(ज) विसंगतियों का पता लगाने में सहायता करने और केंद्र सरकार को रियल टाइम के आधार पर खुफिया जानकारी उपलब्ध कराने में सक्षम बनाने के लिए महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित सभी लॉग; और

(झ) नियम 7 के तहत महत्वपूर्ण दूरसंचार अवसंरचना के लिए विनिर्दिष्ट समय-सीमा में सुरक्षा घटनाओं की रिपोर्टिंग करना।

7. महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित दायित्व

(1) प्रत्येक दूरसंचार कंपनी केंद्र सरकार द्वारा विनिर्दिष्ट प्रारूप और तरीके के माध्यम से निम्नलिखित दायित्वों का अनुपालन सुनिश्चित करेगी:

(क) महत्वपूर्ण दूरसंचार अवसंरचना के संबंध में केंद्र सरकार द्वारा अधिसूचित सुरक्षा उपायों, मानकों, विनिर्देशों और उन्नयन की आवश्यकताओं और प्रक्रियाओं का कार्यान्वयन;

(ख) सॉफ्टवेयर और हार्डवेयर के विवरण, महत्वपूर्ण दूरसंचार अवसंरचना पर और की निर्भरता अथवा केंद्र सरकार के विनिर्देशों के अनुसार कोई अन्य विवरण सहित महत्वपूर्ण दूरसंचार अवसंरचना की सम्पूर्ण सूची का रखरखाव;

(ग) दूरसंचार नेटवर्क आर्किटेक्चर में परिवर्तन सहित महत्वपूर्ण दूरसंचार अवसंरचना के दूरसंचार नेटवर्क आर्किटेक्चर के लॉग और प्रलेखन का संरक्षण;

(घ) महत्वपूर्ण दूरसंचार अवसंरचना के अभिगम के लिए प्राधिकृत सभी कार्मिकों के लिए लागू होने वाली समुचित सत्यापन प्रक्रियाओं और प्रोटोकॉल के लिए योजना बनाने, विकास करने तथा उनका रखरखाव बनाए रखने तथा जैसाकि केंद्र सरकार द्वारा विनिर्देशित है, समय-समय पर उनकी समीक्षा करना;

(ङ) महत्वपूर्ण दूरसंचार अवसंरचना के उपयोग में होने तक उसमें तैनात किए गए दूरसंचार उपकरणों और अन्य उपकरणों की आपूर्ति श्रृंखला के रिकॉर्ड का रखरखाव करना तथा केंद्र सरकार द्वारा जब कभी मांगा जाएगा तब सूचना उपलब्ध कराना;

(च) यह सुनिश्चित करना कि महत्वपूर्ण दूरसंचार अवसंरचना की मरम्मत अथवा रखरखाव के उद्धेश्यों हेतु दूरस्थ अभिगम को जैसी भी स्थिति हो केवल तभी उपलब्ध कराया जा सकता है जब उसके लिए केंद्र सरकार का पूर्व में लिखित अनुमोदन लिया गया हो जिसमें वह स्थल भी शामिल है जहाँ से मरम्मत और रख-रखाव का कार्य किया जाना है;

(छ) यह सुनिश्चित करना कि खंड (च) के तहत दिए गए दूरस्थ अभिगम के हेतु लॉग तब तक संरक्षित रखे जाएँ जब तक कि महत्वपूर्ण दूरसंचार अवसंरचना उपयोग में है और जब भी केंद्र सरकार द्वारा ऐसे लॉग मांगे जाएँ उन्हें प्रस्तुत करना;

(ज) यह सुनिश्चित करना कि महत्वपूर्ण दूरसंचार अवसंरचना के दूरसंचार नेटवर्क संरचना के लिए भेद्यता/खतरा/जोखिम के विश्लेषण को प्रतिवर्ष या केन्द्र सरकार द्वारा यथा विनिर्देशित प्रति फ्रीक्वेंसी के रूप में किया जाता है;

(झ) महत्वपूर्ण दूरसंचार अवसंरचना के संबंध में दूरसंचार कंपनियों द्वारा अपने वेंडर के साथ किए गए सेवा स्तर करार के लिए आवश्यक प्रलेखित प्रक्रियाओं की योजना, विकास, रखरखाव और उनकी समीक्षा करना;

(ञ) महत्वपूर्ण दूरसंचार अवसंरचना की कार्यविधि में सहयोग करने वाले नेटवर्किंग और संचार उपकरणों, सर्वरों, सिस्टम और सेवाओं के लॉग का नियमित बैकअप लेने की प्रक्रिया की योजना बनाना, विकास करना, रख-रखाव करना और उनकी समीक्षा करना;

(ट) डिजास्टर रिकवरी और व्यवसाय को जारी रखने सहित सुरक्षा घटना के रेस्पोंस सिस्टम के लिए मानक प्रचालन प्रक्रियाओं का कार्यान्वयन;

(ठ) सुरक्षा घटना(ओं) के बारे में केंद्र सरकार को ऐसी घटना के घटित होने के दो घंटे के भीतर इस उद्देश्य हेतु यथा विनिर्दिष्ट प्रारूप और तरीके के माध्यम से समय पर सूचित करने के लिए प्रणालियों का कार्यान्वयन; और

(ड) अपने नेटवर्क के भीतर महत्वपूर्ण दूरसंचार अवसंरचना के विभिन्न घटकों से जुड़े ग्रेडेड रिस्क एसेस्मेंट सहित रिस्क रजिस्टर का रखरखाव, महत्वपूर्ण दूरसंचार अवसंरचना के लिए उत्पन्न जोखिमों से नुकसान और गंभीरता की पहचान करना तथा उन्हें कम करने के उपाय और केन्द्र सरकार द्वारा मांगे जाने पर ऐसी सूचना प्रस्तुत करना।

8. महत्वपूर्ण दूरसंचार अवसंरचना के उन्नयन के लिए आवश्यकताएँ

(1) जहां भी महत्वपूर्ण दूरसंचार अवसंरचना से बनने वाले उपकरणों के उन्नयन की आवश्यकता है उस स्थिति में दूरसंचार कंपनी केन्द्र सरकार को ऐसे उन्नयन के लिए परीक्षण रिपोर्टों के विवरण के साथ इस प्रायोजन हेतु केन्द्र सरकार द्वारा विनिर्दिष्ट प्रारूप और तरीके के माध्यम से सूचित करेगी।

(2) उन्नयन से संबंधित किसी भी गतिविधि को केवल केन्द्र सरकार अथवा इस प्रयोजन के लिए केन्द्र सरकार द्वारा प्राधिकृत किसी व्यक्ति द्वारा पूर्व लिखित प्रमाणीकरण के बाद ही किया जाएगा कि उप-नियम (1) के तहत प्रस्तुत ऐसे उन्नयन के लिए परीक्षण रिपोर्ट इस प्रयोजन हेतु केन्द्र सरकार द्वारा विनिर्दिष्ट मानकों के अनुरूप हैं।

(3) केन्द्र सरकार किसी दूरसंचार कंपनी को महत्वपूर्ण दूरसंचार अवसंरचना में किसी उन्नयन का उपयुक्त नियंत्रित प्रक्रिया के तहत परीक्षण करने तथा ऐसे परीक्षणों के परिणामों को केन्द्र सरकार द्वारा विनिर्दिष्ट प्रारूप और तरीके के माध्यम से प्रस्तुत करने का निर्देश भी दे सकती है और दूरसंचार कंपनी इन निर्देशों का अनुपालन करेगी।

(4) दूरसंचार कंपनी जब तक कि संबंधित महत्वपूर्ण दूरसंचार अवसंरचना उपयोग में है तब तक किसी भी उन्नयन से संबंधित रिकॉर्ड और सूचना का संरक्षण सुनिश्चित करेगी और जब भी केन्द्र सरकार द्वारा मांगा जाएगा कंपनी इन रिकॉर्ड को प्रस्तुत करेगी।

9. इन नियमों का डिजिटल कार्यान्वयन

केंद्र सरकार अधिनियम की धारा 53 के अनुपालन के तहत दूरसंचार कंपनी द्वारा केंद्र सरकार को महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित सुरक्षा घटनाओं और अन्य विवरणों की सूचना देने, मुख्य दूरसंचार सुरक्षा अधिकारी द्वारा अपनाई जाने वाली रिपोर्टिंग प्रक्रियाओं और इन नियमों के तहत विनिर्दिष्ट अन्य प्रक्रियाओं और आवश्यकताओं सहित नियमों के डिजिटल कार्यान्वयन के लिए उपयुक्त पद्धति अधिसूचित कर सकती है।

[फा. सं 24-05/2024-यूबीबी]

देवेंद्र कुमार राय, संयुक्त सचिव

MINISTRY OF COMMUNICATIONS

(Department of Telecommunications)

NOTIFICATION

New Delhi, the 28th August, 2024

G.S.R. 521(E).— The following draft rules, 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), are hereby published for the information of all persons likely to be affected thereby and notice is hereby given that the said draft rules shall be taken into consideration after the expiry of a period of thirty days from the date on which copies of this notification as published in the Official Gazette, are made available to the public;

Objections or suggestions, if any, may be addressed to the Joint Secretary (Telecom), Department of Telecommunications, Ministry of Communications, Government of India, Sanchar Bhawan, 20, Ashoka Road, New Delhi- 110001;

The objections or suggestions which may be received from any person with respect to the said draft rules before the expiry of the aforesaid period shall be taken into consideration by the Central Government.

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 designated employee of a telecommunication entity, appointed pursuant to 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) "**rules**" means the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024;

(e) "**security incident**" shall have the meaning as provided under the Telecommunications (Telecom Cyber Security) Rules, 2024; and

(f) "**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.

(2) The words and expressions used in these rules and not defined herein but defined in the Act, shall have the meaning assigned to them in the Act.

3. Applicability

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

(2) To enable notification of Critical Telecommunication Infrastructure, each telecommunication entity shall provide the details of its telecommunication network, telecommunication services, elements of such network and services, and other relevant information including software and hardware, upon request of the Central Government, in the form specified for this purpose.

4. Compliance requirements

(1) A telecommunication entity shall ensure that Critical Telecommunication Infrastructure, including any spares, hardware and software used in such Critical Telecommunication Infrastructure, are in compliance with:

(a) Essential Requirements (ERs), Interface Requirements (IRs), Indian Telecommunication Security Assurance Requirements (ITSARs) and specifications, testing requirements, or conformity assessment 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;

(b) National Security Directive on Telecommunication Sector (NSDTS) as issued by Central Government and as amended from time to time; and

(c) Directives on Communication security certification issued by the Central Government.

(2) A telecommunication entity shall ensure compliance with standards on Critical Telecommunication Infrastructure as may be notified or prescribed 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) A 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

The Chief Telecom Security Officer shall be responsible for the implementation of these rules, and shall provide the following details in respect of Critical Telecommunication Infrastructure to the Central Government in the form and manner as may be specified:

(a) Telecommunication network architecture of Critical Telecommunication Infrastructure;

(b) Authorised personnel having access to Critical Telecommunication Infrastructure;

(c) Inventory of spares, hardware and software related to Critical Telecommunication Infrastructure;

(d) Details of Vulnerability/ Threat/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; and

(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) Each telecommunication entity shall comply with the following obligations, in the form and manner as specified by the Central Government:

(a) implementation of the security measures, standards, specifications and upgradation requirements and procedures, as notified by the Central Government in relation to Critical Telecommunication Infrastructure;

(b) maintenance of a complete list of Critical Telecommunication Infrastructure along with the software and hardware details, dependencies on and of Critical Telecommunication Infrastructure, or any other details in accordance with the directions of the Central Government;

(c) preservation of the logs and documentation of the telecommunication network architecture of the Critical Telecommunication Infrastructure including the changes in such telecommunication network architecture;

(d) planning, development and maintenance of adequate verification practices and protocols applicable for all personnel authorised to have access to Critical Telecommunication Infrastructure, and periodic review of the same as directed by the Central Government;

(e) maintenance of records of the supply chain of the telecommunication equipment and other equipment deployed in the Critical Telecommunication Infrastructure till the Critical Telecommunication Infrastructure is in use, and provide such information as and when sought by the Central Government;

(f) ensuring that remote access to the Critical Telecommunication Infrastructure for the purpose of repair or maintenance as the case may be, is provided only upon prior written approval of the Central Government including the location from where such repair or maintenance may be provided;

(g) ensuring that the logs for the remote access as provided under clause (f) are preserved till the Critical Telecommunication Infrastructure is in use and producing such logs as and when sought by the Central Government;

(h) ensuring that vulnerability/threat/risk analysis for telecommunication network architecture of critical telecommunication infrastructure is carried out annually or as per frequency directed by the Central Government;

(i) planning, development, maintenance and review of documented processes required for service level agreements entered into by the telecommunication entities with their vendors in relation to Critical Telecommunication Infrastructure;

(j) planning, development, maintenance and review of the process of taking regular backup of logs of networking and communication devices, servers, systems and services supporting the functioning of the Critical Telecommunication Infrastructure;

(k) implementation of standard operating procedures for security incident response systems, including disaster recovery and business continuity;

(l) implementation of mechanisms to ensure intimation of security incident(s) to the Central Government, no later than within two hours of occurrence of such incident, in the form and manner as may be specified for this purpose; and

(m) maintenance of 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 by the Central Government.

8. Requirements for upgradation of Critical Telecommunication Infrastructure

(1) Where upgradation of the equipment which form part of the Critical Telecommunication Infrastructure is required, the telecommunication entity shall inform the Central Government, along with details of the test reports for such upgradation, in the form and manner as may be specified by the Central Government for this purpose.

(2) Any upgradation activity shall be undertaken only upon the prior written certification by the Central Government, or any person authorised by the Central Government for this purpose, that the test reports for such upgradation submitted under sub-rule (1) are in compliance with standards specified by the Central Government for this purpose.

(3) The Central Government may also 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, and the telecommunication entity shall comply with such directions.

(4) 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.

9. Digital implementation of these rules

The Central Government, in furtherance of section 53 of the Act, may notify appropriate means for the digital implementation of these rules, including for intimation by telecommunication entity of security incidents and other details in relation to the Critical Telecommunication Infrastructure to the Central Government, reporting procedures to be undertaken by the Chief Telecommunications Security Officer, and other procedures and requirements as specified under these rules.

[F.No.24-05/2024-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.