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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-22112024-258842
CG-DL-E-22112024-258842

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 664] नई दिल्ली, शुक्रवार, नवम्बर 22, 2024/अग्रहायण 1, 1946
No. 664] NEW DELHI, FRIDAY, NOVEMBER 22, 2024/AGRAHAYANA 1, 1946

IndiaCode

संचार मंत्रालय

(दूरसंचार विभाग)

अधिसूचना

नई दिल्ली, 22 नवम्बर, 2024

सा.का.नि. 723(अ).—केन्द्रीय सरकार दूरसंचार (महत्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024 के प्रारूप को, जिसे 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 उक्त अधिनियम की धारा 56 की उप-धारा (1) की अपेक्षानुसार भारत सरकार के संचार मंत्रालय, दूरसंचार विभाग की अधिसूचना संख्या सा.का.नि. 521 (अ), तारीख 28 अगस्त, 2024 द्वारा भारत के राजपत्र, असाधारण, भाग II, खंड 3, उप-खंड (i), तारीख 28 अगस्त, 2024 में प्रकाशित किया गया था, जिसमें इससे प्रभावित होने वाले व्यक्तियों से उक्त अधिसूचना वाले राजपत्र की प्रतियां जनसाधारण को उपलब्ध कराए जाने की तारीख से तीस दिन की अवधि समाप्त होने से पूर्व आपत्तियां और सुझाव आमंत्रित किए गए थे;

और उक्त राजपत्र की प्रतियां तारीख 29 अगस्त, 2024 को जनसाधारण को उपलब्ध करा दी गई थीं;

और केन्द्रीय सरकार द्वारा उक्त प्रारूप नियमों के संबंध में जनसाधारण से प्राप्त आपत्तियों और सुझावों पर विधिवत रूप से विचार किया गया है;

अतः अब केन्द्रीय 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 निम्नलिखित नियम बनाती है, अर्थात:-

1. संक्षिप्त नाम और प्रारंभ - (1) इन नियमों का संक्षिप्त नाम दूरसंचार (महत्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024 है।

(2) ये राजपत्र में उनके 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 नियम 6 के अधीन नियुक्त मुख्य दूरसंचार सुरक्षा अधिकारी अभिप्रेत है;

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

(घ) "पोर्टल" से नियम 10 के उप-नियम (1) के अधीन केन्द्रीय सरकार द्वारा अधिसूचित पोर्टल अभिप्रेत है;

(ङ) "सुरक्षा घटना" का वही अर्थ होगा जो दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 के नियम 2 के उप-नियम (1) के खंड (च) में समनुदेशित है; और

(च) "दूरसंचार इकाई" का वही अर्थ होगा जो दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 के नियम 2 के उप-नियम (1) के खंड (छ) में समनुदेशित है।

(2) उन शब्दों और पदों के, जो इसमें प्रयुक्त हैं और परिभाषित नहीं हैं किन्तु अधिनियम में परिभाषित हैं, के वही अर्थ होंगे जो उनके उस अधिनियम में हैं।

3. लागू होना - (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 उपबंधों के अधीन 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) केन्द्रीय सरकार पोर्टल पर वह प्ररूप और तरीका निर्दिष्ट करेगी जिसमें प्रत्येक दूरसंचार इकाई अपने दूरसंचार नेटवर्क, दूरसंचार सेवाओं तथा ऐसे नेटवर्क और सेवाओं के घटकों का ब्यौरा उपलब्ध कराएगी।

4. अनुपालन आवश्यकताएँ - (1) प्रत्येक दूरसंचार इकाई 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 मानकों का अनुपालन कर रहे हैं, अर्थात:-

(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 केन्द्रीय सरकार द्वारा अधिसूचित किया जाएगा;

परंतु ऐसे मानकों के अभाव में, कोई दूरसंचार इकाई केवल ऐसे महत्वपूर्ण दूरसंचार अवसंरचना का उपयोग कर सकेगी, जिसमें ऐसे महत्वपूर्ण दूरसंचार अवसंरचना में प्रयुक्त कोई भी अतिरिक्त पुर्जे, हार्डवेयर और सॉफ्टवेयर शामिल हैं, जो इस संबंध में केन्द्रीय सरकार द्वारा अधिसूचित सुसंगत मानकों को पूरा करते हों;

(ख) केन्द्रीय सरकार द्वारा जारी दूरसंचार सेक्टर (एनएसडीटीएस) पर राष्ट्रीय सुरक्षा निदेश;

(ग) केन्द्रीय सरकार द्वारा जारी संचार सुरक्षा प्रमाणन पर निदेश।

(घ) महत्वपूर्ण दूरसंचार अवसंरचना पर लागू ऐसे अन्य मानक जिन्हें केन्द्रीय सरकार द्वारा समय-समय पर अधिसूचित किया जा सके।

5. महत्वपूर्ण दूरसंचार अवसंरचना का निरीक्षण - (1) केन्द्रीय सरकार, आदेश द्वारा, अपने कार्मिकों को दूरसंचार इकाइयों की महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित हार्डवेयर, सॉफ़्टवेयर और डेटा के पहुंच और उसका निरीक्षण करने के लिए प्राधिकृत करेगी।

(2) प्रत्येक दूरसंचार इकाई महत्वपूर्ण दूरसंचार अवसंरचना के निरीक्षण के लिए उप-नियम **(1)** के अधीन केन्द्रीय सरकार द्वारा प्राधिकृत किसी भी कार्मिक की पहुंच सुनिश्चित करेगी।

6. मुख्य दूरसंचार सुरक्षा अधिकारी – (1) मुख्य दूरसंचार सुरक्षा अधिकारी इन नियमों के कार्यान्वयन के लिए उत्तरदायी होगा।

(2) केन्द्रीय सरकार पोर्टल पर वह प्ररूप और तरीका निर्दिष्ट करेगी जिससे प्रत्येक दूरसंचार इकाई महत्वपूर्ण दूरसंचार अवसंरचना के संबंध में ब्यौरा उपलब्ध कराएगी, जिसमें निम्नलिखित ब्यौरा शामिल होगा, अर्थात:-

(क) महत्वपूर्ण दूरसंचार अवसंरचना का दूरसंचार नेटवर्क आर्किटेक्चर;

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

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

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

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

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

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

(ज) विसंगतियों का पता लगाने में सहायता करने और केन्द्रीय सरकार को वास्तविक समय के आधार पर आसूचना की जानकारी उपलब्ध कराने में सक्षम बनाने के लिए महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित सभी लॉग; और

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

7. महत्वपूर्ण दूरसंचार अवसंरचना से संबंधित दायित्व- (1) प्रत्येक दूरसंचार इकाई निम्नलिखित दायित्वों का पालन करेगी, अर्थात्: -

(क) नियम 4 के अधीन दिए गए मानकों के अनुपालन सहित महत्वपूर्ण दूरसंचार अवसंरचना की सुरक्षा सुनिश्चित करना;

(ख) सॉफ्टवेयर और हार्डवेयर विवरण के साथ-साथ ऐसे महत्वपूर्ण दूरसंचार अवसंरचना पर निर्भरता के साथ महत्वपूर्ण दूरसंचार अवसंरचना की सम्पूर्ण सूची का रखरखाव;

(ग) ऐसे दूरसंचार नेटवर्क संरचना में परिवर्तन सहित महत्वपूर्ण दूरसंचार अवसंरचना के दूरसंचार नेटवर्क संरचना के लॉग और प्रलेखन का कम से कम दो वर्ष की अवधि के लिए अथवा केन्द्रीय सरकार द्वारा निर्धारित किसी अन्य अवधि के लिए सुरक्षित तरीके से संरक्षित रखना;

(घ) महत्वपूर्ण दूरसंचार अवसंरचना तक पहुँच रखने वाले सभी अधिकृत कार्मिकों के लिए लागू होने वाली पर्याप्त सत्यापन प्रक्रियाओं और प्रोटोकॉल के लिए योजना बनाने, विकास करने तथा उनका रखरखाव बनाए रखने और केन्द्रीय सरकार के निर्देशानुसार उनकी आवधिक पुनर्विलोकन करना;

(ङ) महत्वपूर्ण दूरसंचार अवसंरचना के उपयोग में होने तक दूरसंचार उपकरणों और अन्य उपकरणों की आपूर्ति शृंखला के अभिलेखों का रखरखाव करना तथा केन्द्रीय सरकार द्वारा जैसा और जब मांगे जाने पर ऐसी जानकारी उपलब्ध कराना;

(च) यह सुनिश्चित करना कि महत्वपूर्ण दूरसंचार अवसंरचना की दूरसंचार नेटवर्क संरचना के लिए भेद्यता अथवा खतरा अथवा जोखिम का विश्लेषण प्रतिवर्ष अथवा ऐसे अंतरालों पर किया जाता है जैसा कि केन्द्रीय सरकार द्वारा निदेशित किया गया है;

(छ) महत्वपूर्ण दूरसंचार अवसंरचना के संबंध में दूरसंचार इकाइयों द्वारा अपने वेंडर के साथ किए गए सेवा स्तर करारों (एसएलए) के लिए आवश्यक प्रक्रियाओं की योजना बनाना, उनका विकास करना, रखरखाव करना और पुनर्विलोकन करना;

(ज) महत्वपूर्ण दूरसंचार अवसंरचना के कार्य में सहायक नेटवर्किंग और संचार उपकरणों, सर्वरों, प्रणालियों और सेवाओं के लॉग का नियमित बैकअप लेने की प्रक्रियाओं की योजना बनाना, विकसित करना, रखरखाव करना और पुनर्विलोकन करना;

(झ) डिजास्टर रिकवरी और व्यवसाय निरंतरता सहित सुरक्षा घटना प्रतिक्रिया प्रणालियों के लिए मानक प्रचालन प्रक्रियाओं का कार्यान्वयन;

(ञ) सुरक्षा घटना(ओं) के बारे में केन्द्रीय सरकार को ऐसी घटना के घटित होने के छः घंटे के भीतर पोर्टल पर यथा विनिर्दिष्ट विधि और प्रक्रिया से सुनिश्चित करने के लिए तंत्र को कार्यान्वित करना; और

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

(2) जहां किसी दूरसंचार इकाई को भारत के क्षेत्र के बाहर किसी स्थान से मरम्मत अथवा रखरखाव के उद्देश्य से अपने महत्वपूर्ण दूरसंचार अवसंरचना तक दूरस्थ पहुंच की आवश्यकता होती है तो वह ऐसा केवल ऐसे स्थान से करेगी जिसके लिए उसने केन्द्रीय सरकार से पूर्व लिखित अनुमोदन प्राप्त किया है और वह ऐसी दूरस्थ पहुंच के प्रत्येक कार्य के लिए –

(क) पोर्टल पर विनिर्दिष्ट विधि और प्रक्रिया से केंद्र सरकार को ऐसी दूरस्थ पहुंच की उचित सूचना प्रदान करेगी; और

(ख) यह सुनिश्चित करेगी कि ऐसी दूरस्थ पहुंच के लिए लॉग को कम से कम एक वर्ष के लिए संरक्षित किए जाते हैं और केन्द्रीय सरकार द्वारा मांगे जाने पर प्रदान किए जाते हैं।

(3) प्रत्येक दूरसंचार इकाई उप-नियम (1) के अधीन अपने द्वारा की गई कार्रवाई से संबंधित एक विस्तृत रिपोर्ट को पोर्टल पर विनिर्दिष्ट विधि और प्रक्रिया से प्रस्तुत करेगी।

(4) केन्द्रीय सरकार उप-नियम (3) के अधीन किसी दूरसंचार इकाई से प्राप्त किसी भी रिपोर्ट अथवा अन्य जानकारी के अनुसरण में, -

(क) ऐसी दूरसंचार इकाई से आगे स्पष्टीकरण मांग सकती है; अथवा

(ख) महत्वपूर्ण दूरसंचार अवसंरचना की सुरक्षा या ऐसी अवसंरचना के लिए जोखिम को कम करने के लिए ऐसी दूरसंचार इकाई को कोई विनिर्देश, आदेश या अनुदेश जारी करना।

8. महत्वपूर्ण दूरसंचार अवसंरचना के उन्नयन के लिए आवश्यकताएँ- (1) जहां महत्वपूर्ण दूरसंचार अवसंरचना का भाग बनने वाले उपकरणों का उन्नयन अपेक्षित है वहां दूरसंचार इकाई ऐसे उन्नयन के लिए परीक्षण रिपोर्ट के विवरण सहित केन्द्रीय सरकार को उस विधि और प्रक्रिया से सूचित करेगी जैसा केन्द्रीय सरकार द्वारा इस प्रयोजन के लिए विनिर्दिष्ट किया जाए।

(2) केन्द्रीय सरकार उप-नियम **(1)** के अधीन आवेदन प्राप्त होने के चौदह दिनों के भीतर –

(क) यदि आवश्यक हो तो दूरसंचार इकाई से कोई और स्पष्टीकरण मांगेगी;

(ख) उप-नियम (3) के अधीन आगे परीक्षण करने के लिए ऐसी इकाई को विनिर्देश जारी करेगी; अथवा

(ग) उन्नयन गतिविधि के लिए आवेदन को स्वीकृत या अस्वीकार करेगी।

(3) केन्द्रीय सरकार किसी दूरसंचार इकाई को महत्वपूर्ण दूरसंचार अवसंरचना में किसी उन्नयन का समुचित नियंत्रित प्रक्रिया के अधीन परीक्षण करने तथा ऐसे परीक्षणों के परिणामों को केन्द्रीय सरकार द्वारा विनिर्दिष्ट विधि और प्रक्रिया से प्रस्तुत करने का विनिर्देश भी दे सकेगी और दूरसंचार इकाई ऐसे विनिर्देशों का अनुपालन करेगी।

(4) जहां केन्द्रीय सरकार ऐसे आवेदन की प्राप्ति की तारीख से चौदह दिन की अवधि के भीतर उप-नियम (2) के अधीन कोई स्पष्टीकरण नहीं मांगती है अथवा निर्देश जारी नहीं करती है अथवा अपना अनुमोदन अथवा अस्वीकृति निर्दिष्ट नहीं करती है, वहां दूरसंचार इकाई ऐसे उन्नयन कार्यकलाप के साथ आगे बढ़ सकती है:

परंतु जहां केन्द्रीय सरकार ने उप-नियम (2) के अधीन स्पष्टीकरण मांगा है, वहां चौदह दिनों की ऐसी अवधि ऐसी दूरसंचार इकाई द्वारा स्पष्टीकरण प्रस्तुत करने की तारीख से मानी जाएगी:

परंतु यह और कि जहां केन्द्रीय सरकार ने उप-नियम (3) के अधीन उन्नयन का परीक्षण करने का निर्देश दिया है, वहां चौदह दिनों की ऐसी अवधि ऐसे परीक्षणों के परिणामों को प्रस्तुत करने की तारीख से मानी जाएगी जैसा कि केन्द्रीय सरकार द्वारा सुरक्षित मोड के माध्यम से मामले दर मामले के आधार पर विनिर्दिष्ट किया जा सकता है।

(5) जहां किसी सुरक्षा घटना के प्रतिकूल प्रभावों का पता लगाने अथवा कम करने के लिए उन्नयन आवश्यक है, वहां दूरसंचार इकाई उप-नियम (1) के अधीन आवेदन किए बिना महत्वपूर्ण दूरसंचार अवसंरचना का हिस्सा बनने वाले किसी भी उपकरण के सॉफ्टवेयर या हार्डवेयर में तत्काल उन्नयन कर सकती है और ऐसे उन्नयन के चौबीस घंटे के भीतर केन्द्रीय सरकार को उस विधि और प्रक्रिया से रिपोर्ट कर सकती है, जैसा कि केन्द्रीय सरकार निम्न सुसंगत विवरण के साथ निर्धारित कर सकती है-

(क) संबंधित सुरक्षा घटना का विवरण; और

(ख) उन्नयन की आवश्यकता वाले उपकरण का प्रासंगिक सॉफ्टवेयर अथवा हार्डवेयर और ऐसे उपकरण के संबंध में किए गए उन्नयन की प्रकृति।

(6) केन्द्रीय सरकार उप-नियम (5) के अधीन सूचना प्राप्त होने पर दूरसंचार इकाई से आगे की जानकारी या स्पष्टीकरण मांग सकती है अथवा आगे के परीक्षण और रिपोर्टिंग के लिए निर्देश जारी कर सकती है जैसा कि वह आवश्यक समझे।

(7) दूरसंचार इकाई किसी भी उन्नयन से संबंधित अभिलेखों और सूचनाओं का संरक्षण सुनिश्चित करेगी जब तक कि सुसंगत महत्वपूर्ण दूरसंचार अवसंरचना उपयोग में है और ऐसे अभिलेखों को केन्द्रीय सरकार द्वारा मांगे जाने पर प्रस्तुत किया जाएगा।

(8) इस नियम में कोई भी बात ऐसे नियमित सॉफ्टवेयर अद्यतन पर लागू नहीं होगी जिसका उद्देश्य महत्वपूर्ण दूरसंचार अवसंरचना के कार्यनिष्पादन अथवा सुरक्षा में क्रमिक सुधार करना हो।

9. नियमों का उल्लंघन. -- अन्यथा उपबंधित के सिवाय इन नियमों के उपबंधों के किसी भी उल्लंघन से अधिनियम के प्रावधानों के अनुसार निपटा जाएगा।

10. डिजिटल कार्यान्वयन. - (1) केन्द्रीय सरकार इन नियमों के डिजिटल कार्यान्वयन के प्रयोजन के लिए एक पोर्टल अधिसूचित करेगी और कोई अन्य कार्यान्वयन प्रणाली भी विनिर्दिष्ट कर सकेगी।

(2) जहां केन्द्रीय सरकार दूरसंचार इकाइयों को कोई आदेश, निर्देश अथवा अनुदेश जारी करने के लिए अथवा ऐसी दूरसंचार इकाइयों से कोई सूचना एकत्रित करने के लिए पोर्टल के अतिरिक्त संचार के किसी अन्य सुरक्षित तरीके का उपयोग करना आवश्यक समझती है वहां वह मामले दर मामले आधार पर संचार के ऐसे सुरक्षित तरीके का उपयोग कर सकती है।

(3) प्रत्येक दूरसंचार इकाई पोर्टल का उपयोग करके अथवा केन्द्रीय सरकार द्वारा निर्धारित संचार के सुरक्षित तरीके के माध्यम से इन नियमों के अधीन केन्द्रीय सरकार को सूचना देने अथवा प्रस्तुत करने से संबंधित दायित्वों का अनुपालन सुनिश्चित करेगी।

[फा. सं. 24-08/2024-यूबीबी]

देवेंद्र कुमार राय, संयुक्त सचिव

IndiaCode

MINISTRY OF COMMUNICATIONS

(Department of Telecommunications)

NOTIFICATION

New Delhi, the 22nd November, 2024

G.S.R. 723(E).—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 29^{th} 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;

(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.

[F. No. 24-08/2024-UBB]

DEVENDRA KUMAR RAI, Jt. Secy.

IndiaCode

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. SARVESH KUMAR SRIVASTAVA Digitally signed by SARVESH KUMAR SRIVASTAVA Date: 2024.11.22 21:31:21 +05'30'