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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-21112024-258808
CG-DL-E-21112024-258808

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 661] नई दिल्ली, बृहस्पतिवार, नवम्बर 21, 2024/कार्तिक 30, 1946
No. 661] NEW DELHI, THURSDAY, NOVEMBER 21, 2024/KARTIKA 30, 1946

संचार मंत्रालय

(दूरसंचार विभाग)

अधिसूचना

नई दिल्ली, 21 नवम्बर, 2024

सा.का.नि. 720(अ).—दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 का प्रारूप जिसे केंद्रीय सरकार, दूरसंचार अधिनियम, 2023 (2023 का 44) की धारा 56 की उपधारा (2) के खंड (फ) के साथ पठित धारा 22 की उपधारा (1) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए बनाने का प्रस्ताव करती है, उक्त अधिनियम की धारा 56 की उपधारा (1) की अपेक्षा के अनुसार भारत के राजपत्र, असाधारण, भाग II खंड 3, उपखंड (i), तारीख 28 अगस्त, 2024 में, भारत सरकार के संचार मंत्रालय के दूरसंचार विभाग की अधिसूचना संख्या सा.का.नि. 520(अ), तारीख 28 अगस्त, 2024 द्वारा उन सभी व्यक्तियों से जिनके उससे प्रभावित होने की संभावना है, ऐसी तारीख से जिसको उक्त अधिसूचना से युक्त राजपत्र की प्रतियां जनसाधारण को उपलब्ध करवाई गई थीं, तीस दिवस की अवधि की समाप्ति से पूर्व आक्षेप और सुझाव आमंत्रित करते हुए प्रकाशित किया गया था;

उक्त राजपत्र की प्रतियां जनसाधारण को तारीख 29 अगस्त, 2024 को उपलब्ध करवाई गई थीं;

उक्त प्रारूप नियमों के संबंध में जनसाधारण से प्राप्त आक्षेपों और सुझावों पर केंद्रीय सरकार द्वारा सम्यक् रूप से विचार किया गया है;

अतः अब केन्द्रीय सरकार, दूरसंचार अधिनियम, 2023 (2023 का 44) की धारा 56 की उपधारा (2) के खंड (फ) के साथ पठित धारा 22 की उपधारा (1) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए और मोबाईल डिवाईस उपस्कर पहचान संख्या से छेड़छाड़ की रोकथाम नियम, 2017 को उन बातों के सिवाय अधिक्रांत करते हुए, जिन्हें ऐसे अधिक्रमण से पूर्व किया गया है या करने का लोप किया गया है तथा इन नियमों के अधीन की गई कार्रवाई के निबंधनों और शर्तों जिसके अधीन इसके अनुसरण में किए गए रजिस्ट्रीकरण भी है, को अध्यारोही किए बिना निम्नलिखित नियम बनाती है, अर्थात्:

अध्याय 1

प्रारंभिक

1. संक्षिप्त नाम और प्रारंभ:- (1) इन नियमों का संक्षिप्त नाम दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 है।

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

2. परिभाषाएँ- (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) "प्रमाणित अभिकरण" से सुरक्षा संपरीक्षा करने के लिए पोर्टल पर केंद्रीय सरकार द्वारा विनिर्दिष्ट अभिकरण अभिप्रेत है।

(ग) "मुख्य दूरसंचार सुरक्षा अधिकारी" से नियम 6 के अधीन नियुक्त दूरसंचार इकाई के अभिहित कर्मचारी अभिप्रेत है।

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

(ङ) "सुरक्षा घटना" से ऐसी घटना अभिप्रेत है जिसका दूरसंचार साइबर सुरक्षा पर वास्तविक या संभावित जोखिम हो;

(च) "दूरसंचार साइबर सुरक्षा" से दूरसंचार नेटवर्क और दूरसंचार सेवाओं की साइबर सुरक्षा अभिप्रेत है जिसमें उपकरण, नीति, सुरक्षा, अवधारणा, सुरक्षा रक्षोपाय, मार्गदर्शक सिद्धांत, जोखिम प्रबंधन दृष्टिकोण, कार्रवाई, आश्वासन और प्रौद्योगिकी सम्मिलित हैं जिनका उपयोग साइबर पर्यावरण में सुसंगत सुरक्षा जोखिमों के लिए दूरसंचार नेटवर्क और दूरसंचार सेवाओं की सुरक्षा के लिए किया जा सकता है;

(छ) “दूरसंचार इकाई” से इस अधिनियम की धारा 3 की उप-धारा (।) के अधीन प्राधिकार प्राप्त प्राधिकृत इकाई अथवा इस अधिनियम की धारा 3 की उप-धारा (3) के अधीन प्राधिकार की अपेक्षा से छूट प्राप्त व्यक्ति सहित दूरसंचार सेवाएं उपलब्ध कराने अथवा दूरसंचार नेटवर्क स्थापित करने, उसका प्रचालन, रखरखाव अथवा विस्तार करने वाला कोई व्यक्ति अभिप्रेत है।

(ज) “दूरसंचार उपस्कर पहचान संख्या” से निम्नलिखित दूरसंचार पहचान संख्या अभिप्रेत है:

i) अंतरराष्ट्रीय मोबाइल उपस्कर पहचान संख्या (आईएमईआई); या

ii) इलेक्ट्रॉनिक क्रम संख्या (ईएसएन); या

iii) अन्य कोई संख्या या संकेत जो विशिष्ट दूरसंचार उपस्कर की पहचान करता है।

(2) उन शब्दों और पदों के, जो इन नियमों में प्रयुक्त हैं और परिभाषित नहीं है किंतु अधिनियम में परिभाषित हैं, वही अर्थ होंगे, जो उनके इस अधिनियम में है।

3. डेटा संग्रह, साझा करना और विश्लेषण

(1) केंद्रीय सरकार या केंद्रीय सरकार द्वारा सुरक्षा और दूरसंचार साइबर सुरक्षा सुनिश्चित करने के प्रयोजनार्थ प्राधिकृत कोई अभिकरण :

(क) केन्द्रीय सरकार द्वारा पोर्टल पर यथा विनिर्दिष्ट तरीके से अथवा स्वरूप में दूरसंचार संस्था से ट्रैफिक डेटा और संदेशों के कंटेन्ट के अलावा किसी भी अन्य डेटा की मांग कर सकती है; और

(ख) दूरसंचार संस्था को विनिर्दिष्ट पॉइंट से इस प्रकार के डेटा के प्रसंस्करण और भंडारण के लिए इसका संग्रह करने और उसे उपलब्ध कराने के लिए आवश्यक अवसंरचना और उपस्कर संस्थापित करने का निदेश दे सकती है।

(2) उप-नियम (1) के अधीन संग्रहित डेटा का विश्लेषण दूरसंचार साइबर सुरक्षा बढ़ाने के उपाय करने के लिए किया जा सकता है और दूरसंचार साइबर सुरक्षा प्रयोजन से और दूरसंचार साइबर सुरक्षा सुनिश्चित करने के लिए केंद्रीय सरकार ऐसे विश्लेषण को अवधारित सीमा तक-

(क) विधि प्रवर्तन और सुरक्षा संबंधी क्रियाकलापों में सम्मिलित केंद्रीय सरकार की किसी भी अभिकरण को उपलब्ध करा सकती है; और

(ख) दूरसंचार इकाईयों या उपयोक्ताओं के साथ शेयर कर सकती है;

परंतु इस प्रकार प्रसारित या साझा किए गए किसी भी डेटा का उपयोग दूरसंचार साइबर सुरक्षा सुनिश्चित करने के अलावा किसी अन्य प्रयोजन के लिए नहीं किया जाएगा।

(3) केंद्रीय सरकार और इन नियमों के अधीन डेटा संग्रह करने के लिए केंद्रीय सरकार द्वारा प्राधिकृत कोई अभिकरण और साथ ही ऐसे व्यक्ति जिनके साथ उप-नियम (2) के अधीन इस प्रकार का डेटा शेयर किया जाता है पर्याप्त सुरक्षा संबंधी उपाय करेंगे जिसमें केन्द्रीय सरकार द्वारा विनिर्दिष्ट किए गए कुछ सुरक्षा संबंधी उपाय शामिल है ताकि यह सुनिश्चित किया जा सके कि ऐसे डेटा सख़्त गोपनीयता के साथ भंडारित और अनुरक्षित किये जाएँ और उस तक किसी भी अप्राधिकृत पहुँच को रोका जा सके।

4. दूरसंचार साइबर सुरक्षा संबंधी दायित्व- (1) कोई भी व्यक्ति

(क) दूरसंचार साइबर सुरक्षा को खतरे में नहीं डालेगा; अथवा

(ख) ऐसा मैसेज नहीं भेजेगा जो दूरसंचार साइबर सुरक्षा को प्रतिकूल ढ़ग से प्रभावित करता हो।

(2) उप-नियम (1) की व्यापकता पर प्रतिकूल प्रभाव डाले बिना, कोई भी व्यक्ति दूरसंचार उपस्कर या दूरसंचार पहचान संख्या या दूरसंचार नेटवर्क या दूरसंचार सेवाओं के दुरुपयोग द्वारा या निम्नलिखित के द्वारा दूरसंचार साइबर सुरक्षा को खतरे में नहीं डालेगा:

(क) कपट, छल या प्रतिरूपण;

(ख) किसी भी ऐसे संदेश को प्रेषित करना जो कपट पर आधारित हो;

(ग) किसी भी सुरक्षा घटना कारित करना या सुरक्षा घटना कारित करने का आशय रखना, या

(घ) ऐसे किसी अन्य उपयोग में लिप्त होना जो तत्समय प्रवृत्त किसी अन्य विधि के किसी भी उपबंध के विपरीत हो।

(ड.) कोई अन्य रीति जिससे दूरसंचार साइबर सुरक्षा पर जोखिम हो सकता हो।

(3) प्रत्येक दूरसंचार इकाई दूरसंचार साइबर सुरक्षा सुनिश्चित करने के लिए दूरसंचार पहचान संख्याओं या दूरसंचार उपस्करों या दूरसंचार नेटवर्क या दूरसंचार सेवाओं के दुरुपयोग की रोकथाम के लिए केंद्रीय सरकार द्वारा जारी किए जा सकने वाले निदेशों और मानकों, जिनमें उनके कार्यान्वयन के लिए समयसीमा भी शामिल है, का अनुपालन सुनिश्चित करेगी।

(4) प्रत्येक दूरसंचार इकाई दूरसंचार साइबर सुरक्षा सुनिश्चित करने के लिए निम्नलिखित उपायों का कार्यान्वयन सुनिश्चित करेगी, अर्थात:-

(क) दूरसंचार साइबर सुरक्षा नीति अपनाएगी, जिसमें निम्नलिखित सम्मिलित होंगे:

(i) दूरसंचार साइबर सुरक्षा को बढ़ाने के लिए रक्षोपाय, जोखिम प्रबंधन दृष्टिकोण, कार्रवाई, प्रशिक्षण, सर्वोत्तम प्रणाली और प्रौद्योगिकी;

(ii) दूरसंचार नेटवर्क परीक्षण जिसमें कठोरता, भेद्यता निर्धारण और भेदन परीक्षण शामिल हैं;

(iii) जोखिम निर्धारण, पहचान और सुरक्षा घटनाओं की रोकथाम;

(iv) सुरक्षा घटनाओं से निपटने के लिए त्वरित कार्रवाई प्रणाली जिसमें ऐसी घटनाओं के प्रभाव को सीमित करने के लिए शमन उपाय सम्मिलित हैं; और

(v) ऐसी घटनाओं से सीख सुनिश्चित करने और दूरसंचार साइबर सुरक्षा को और सुदृढ़ करने के लिए सुरक्षा घटनाओं का फोरेंसिक विश्लेषण;

(ख) उप-खंड (क) के अधीन निर्दिष्ट नीति को अपनाने पर केंद्रीय सरकार को इस प्रकार सूचित करेगी जैसा केंद्रीय सरकार द्वारा अवधारित किया जाए;

(ग) सुरक्षा घटनाओं के जोखिमों की पहचान करना और उन्हें कम करना और ऐसी घटनाओं पर समय पर प्रतिक्रिया सुनिश्चित करना;

(घ) सुरक्षा घटनाओं के समाधान के लिए उचित कार्रवाई करना और उनके प्रभाव को कम करना;

(ङ) दूरसंचार साइबर सुरक्षा पर केंद्रीय सरकार द्वारा जारी किए गए निदेशों और मानकों का कार्यान्वयन सुनिश्चित करना;

(च) दूरसंचार साइबर सुरक्षा के प्रति खतरों के प्रति समुत्थान शक्ति का निर्धारण करने के लिए अपने स्वयं के तंत्र के माध्यम से और प्रमाणित अभिकरण के माध्यम से अपने नेटवर्क की ऐसे अंतरालों पर कालिक दूरसंचार साइबर सुरक्षा संपरीक्षा करना जैसा केंद्रीय सरकार द्वारा पोर्टल पर निर्दिष्ट किया जाए और संपरीक्षा रिपोर्ट को केंद्रीय सरकार के साथ साझा करना जो आवश्यकता पड़ने पर आगे की संपरीक्षा कर सकती है;

(छ) सुरक्षा घटना की सूचना केंद्रीय सरकार या केंद्रीय सरकार द्वारा इस निमित्त प्राधिकृत किसी भी अधिकारी को देना और नियम 7 में निर्दिष्ट तरीके से ऐसी घटनाओं से निपटने के लिए किए गए उपाय करना;

(ज) उप-नियम (3) के अधीन केंद्रीय सरकार द्वारा विनिर्दिष्ट समयावधि के भीतर स्वयं अथवा अन्य दूरसंचार इकाईयों के सहयोग से सुरक्षा प्रचालन केंद्र (एसओसी) जैसी सुविधाएं स्थापित करना ताकि निम्नलिखित का समाधान किया जा सके अर्थात्:

(i) दूरसंचार साइबर सुरक्षा और सुरक्षा घटनाओं, घुसपैठ और दूरसंचार सेवाओं अथवा दूरसंचार नेटवर्क के भंग के साथ-साथ ऐसी घटनाओं, घुसपैठ या भंग के प्रयास के कारण की निगरानी करना;

(ii) दूरसंचार सेवा या दूरसंचार नेटवर्क को प्रभावित करने वाले खतरे के कारकों के ब्यौरे बनाए रखना;

(iii) प्रचालन और रखरखाव के कमांड लॉग बनाए रखना;

(iv) सुरक्षा प्रचालन केंद्र (एसओसी) (फ़ायरवॉल, घुसपैठ का पता लगाने वाली प्रणाली (आईडीएस) या घुसपैठ रोकथाम प्रणाली (आईपीएस), या सुरक्षा सूचना और घटना प्रबंधन (एसआईईएम) या ऐसे अन्य समाधान) के लॉग बनाए रखना;

(v) दूरसंचार सेवा या दूरसंचार नेटवर्क की सुरक्षा के लिए आवश्यक दूरसंचार सेवाओं या दूरसंचार नेटवर्क के घटकों या अन्य घटकों के लॉग बनाए रखना;

(vi) केंद्रीय सरकार द्वारा पोर्टल पर विनिर्दिष्ट अवधि के लिए इस उप-नियम में विनिर्दिष्ट सभी रिकॉर्ड या लॉग का रख-रखाव करना और केंद्रीय सरकार द्वारा इस निमित्त प्राधिकृत व्यक्ति को उपलब्ध कराना; और

(vii) सुरक्षा घटनाओं से संबंधित जांच के प्रयोजन के लिए विधि प्रवर्तन एजेंसियों सहित केंद्रीय सरकार द्वारा प्राधिकृत व्यक्ति को आवश्यक सहायता प्रदान करना।

(5) प्रत्येक दूरसंचार इकाई उप-नियम (4) के अधीन अपने द्वारा की गई कार्रवाई से संबंधित विस्तृत रिपोर्ट पोर्टल पर विनिर्दिष्ट प्ररूप और रीति में प्रस्तुत करेगी।

(6) केंद्रीय सरकार उपनियम (4) के अधीन किसी दूरसंचार इकाई से प्राप्त किसी रिपोर्ट या अन्य सूचना के अनुसरण में -

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

(ख) दूरसंचार साइबर सुरक्षा के संरक्षण के लिए और दूरसंचार साइबर सुरक्षा के लिए जोखिम को कम करने के लिए ऐसी दूरसंचार इकाई को कोई निदेश, आदेश या अनुदेश जारी कर सकती है।

5. दूरसंचार साइबर सुरक्षा को संरक्षित करने और सुनिश्चित करने के उपाय - (1) केंद्रीय सरकार, जैसा वह आवश्यक समझे, डिजिटल और अन्य तंत्र स्थापित कर सकती है ताकि ऐसे कार्यों की पहचान की जा सके या किसी व्यक्ति को उनकी पहचान करने और रिपोर्ट करने में सक्षम बनाया जा सके, जो दूरसंचार साइबर सुरक्षा को खतरा पहुंचा सकते हैं।

(2) केंद्रीय सरकार, उप-नियम (1) के अधीन प्राप्त सूचना की जांच के पश्चात्, उस दूरसंचार पहचान संख्या की पहचान करेगी जिसके उपयोग से दूरसंचार साइबर सुरक्षा को खतरा उत्पन्न होने का आरोप है तथा उस व्यक्ति की भी पहचान करेगी जिसे दूरसंचार इकाई द्वारा ऐसी दूरसंचार पहचान संख्या जारी की गई है और ऐसे व्यक्ति को उसके ब्यौरे सहित नोटिस जारी करेगी।

(3) वह व्यक्ति जिसे उप-नियम (2) के अधीन नोटिस जारी किया जाता है, ऐसे नोटिस की प्राप्ति के सात दिन के भीतर केंद्रीय सरकार को लिखित प्रत्युत्तर भेजेगा और यदि ऐसी अवधि के भीतर कोई प्रत्युत्तर प्राप्त नहीं होता है तो केंद्रीय सरकार उप-नियम (5) के अधीन आदेश जारी करने के लिए कार्रवाई करेगी।

(4) यदि उपनियम (2) के अधीन नोटिस के प्राप्तकर्ता से उपनियम (3) में विनिर्दिष्ट समय के भीतर प्रत्युत्तर प्राप्त होता है, तो केंद्रीय सरकार ऐसे व्यक्ति को सुनवाई का उचित अवसर देने के पश्चात् उपनियम (5) के अधीन जैसा वह ठीक समझे उस पर आदेश पारित करेगी।

(5) केंद्रीय सरकार तथ्यों के अपने निर्धारण और उस व्यक्ति द्वारा जिसे उप-नियम (2) के अधीन नोटिस जारी किया गया है, किए गए निवेदन, यदि कोई हो, के आधार पर कारणों को अभिलिखित करते हुए एक आदेश पारित करेगी, जिसमें दूरसंचार इकाई को प्रदत्त निदेश शामिल हो सकते हैं कि—

(क) ऐसे आदेश में विनिर्दिष्ट रीति से और अवधि के लिए संबंधित दूरसंचार पहचान संख्या के उपयोग को अस्थायी रूप से निलंबित कर सकती है; या

(ख) संबंधित दूरसंचार पहचान संख्या के उपयोग को स्थायी रूप से समाप्त कर सकती है।

(6) जहां केंद्रीय सरकार समझती है कि उपनियम (5) के अधीन तत्काल कार्रवाई लोकहित में आवश्यक या समीचीन है, वहां वह उपनियम (2) के अधीन नोटिस जारी किए बिना, कारणों को अभिलिखित करते हुए एक आदेश पारित करेगी, जिसमें दूरसंचार इकाई को संबंधित दूरसंचार पहचानकर्ता के उपयोग को अस्थायी रूप से निलंबित करने के लिए उचित निदेश दिए जाएंगे।

(7) यथास्थिति उप-नियम (5) या उप-नियम (6) के अधीन आदेश की एक प्रति, उप-नियम (2) में विनिर्दिष्ट व्यक्ति या उप-नियम (6) में विनिर्दिष्ट दूरसंचार इकाई या आदेश से प्रभावित ऐसे व्यक्ति को प्रदान की जाएगी और यथास्थिति ऐसा व्यक्ति या, दूरसंचार इकाई, आदेश जारी करने की तारीख से तीस दिनों की अवधि के भीतर लिखित रूप में केंद्रीय सरकार को कारणों के साथ प्रस्तुत कर सकती है कि ऐसी कार्रवाई क्यों नहीं की जानी चाहिए।

(8) केंद्रीय सरकार, उस व्यक्ति को, जिसे उप-नियम (7) के अधीन आदेश की प्रति उपलब्ध कराई गई है, सुनवाई का उचित अवसर देने के पश्चात् और कारणों को लेखबद्ध करके उप-नियम (5) या उप-नियम (6) के अधीन पारित आदेश को या तो बनाए रखने या उपांतरित करने या वापस लेने का आदेश पारित करेगी:

परन्तु उप-नियम (6) के अधीन आदेश के किसी भी संशोधन में दूरसंचार इकाई को उप-नियम (5) के खंड (ख) के अधीन निर्दिष्ट सुसंगत दूरसंचार पहचान संख्या के उपयोग को स्थायी रूप से समाप्त करने का निदेश देने वाला आदेश भी शामिल हो सकता है।

(9) उप-नियम (5), उप-नियम (6) या उप-नियम (8) के अधीन संबंधित दूरसंचार पहचान संख्या के उपयोग के निलंबन या स्थायी रूप से समाप्त करने का कोई आदेश उस व्यक्ति से जुड़े अन्य दूरसंचार उपस्कर या दूरसंचार पहचान संख्या पर भी लागू किया जा सकेगा, जिसे दूरसंचार पहचान संख्या उप-नियम (2) के अधीन पहचाना गया है या उप-नियम (2) के अधीन पहचाने गए व्यक्ति को जारी की गई अन्य दूरसंचार पहचान संख्याओं पर भी लागू किया जा सकेगा।

(10) केंद्रीय सरकार ऐसे व्यक्तियों और दूरसंचार पहचान संख्याओं का संग्रह रख सकेगी जिन पर उप-नियम (5) या उप-नियम (6) या उप-नियम (8) या उप-नियम (9) के अधीन आदेशों के अनुसरण में कार्रवाई की गई है और दूरसंचार इकाईयों को ऐसे आदेश की तारीख से अधिकतम तीन वर्ष की अवधि के लिए ऐसे व्यक्तियों के लिए दूरसंचार सेवा तक पहुंच को प्रतिषिद्ध या सीमित करने का निदेश दे सकेगी।

(11) केंद्रीय सरकार यदि वह आवश्यक समझे या दूरसंचार पहचान संख्याओं से जुड़ी सेवाएं प्रदान करने वाले किसी व्यक्ति द्वारा किए गए किसी अनुरोध के अनुसरण में उप-नियम (5) या उप-नियम (6) या उप-नियम (8) या उप-नियम (9) के अधीन आदेशों के अनुसरण में ऐसी दूरसंचार पहचान संख्याओं, जिन पर कार्रवाई की गई है, की सूची ऐसे व्यक्तियों के साथ साझा कर सकेगी और आदेश द्वारा ऐसे व्यक्तियों को निदेश दे सकेगी कि वे अपने उपभोक्ताओं की पहचान के लिए या सेवाओं के वितरण के लिए ऐसी दूरसंचार पहचान संख्याओं के उपयोग को उस तरीके से प्रतिषिद्ध या परिसीमित करें, जैसा कि ऐसे आदेश में विनिर्दिष्ट किया जाए।

(12) ऐसी भी दूरसंचार पहचान संख्या को, जो इस नियम के अनुसार दूरसंचार सेवा के निलंबन या स्थायी समाप्ति का विषय है, ऐसे आदेश जारी होने अथवा स्थायी समाप्ति की तारीख से एक (1) वर्ष की अवधि के लिए जिसे विशिष्ट मामलों में तीन (3) वर्ष तक बढ़ाया जा सकता है, किसी अन्य व्यक्ति को पुनः आवंटित नहीं किया जाएगा।

6. मुख्य दूरसंचार सुरक्षा अधिकारी - (1) प्रत्येक दूरसंचार इकाई एक मुख्य दूरसंचार सुरक्षा अधिकारी नियुक्त करेगा जिसका ब्यौरा ऐसे प्ररूप में केन्द्रीय सरकार को लिखित रूप में उपलब्ध कराया जाएगा जैसा पोर्टल पर विनिर्दिष्ट किया जाए। ऐसे अधिकारी के किसी प्रतिस्थापन या परिवर्तन की सूचना तत्काल केन्द्रीय सरकार को ऐसे प्ररूप में दी जाएगी, जैसा कि सरकार द्वारा पोर्टल पर विनिर्दिष्ट किया जाए।

(2) मुख्य दूरसंचार सुरक्षा अधिकारी भारत का नागरिक और निवासी होगा तथा दूरसंचार इकाई के निदेशक मंडल या समान शासी निकाय के प्रति उत्तरदायी होगा।

(3) मुख्य दूरसंचार सुरक्षा अधिकारी इन नियमों के कार्यान्वयन के लिए दूरसंचार इकाई की ओर से केंद्रीय सरकार के साथ समन्वय करने के लिए उत्तरदायी होगा, जिसमें नियम **7** के अधीन किसी भी रिपोर्टिंग अपेक्षाओं या सुरक्षा घटनाओं की रिपोर्टिंग का अनुपालन भी शामिल है।

7. सुरक्षा घटनाओं की रिपोर्टिंग-(1) **दूरसंचार इकाई-**

(क) अपने दूरसंचार नेटवर्क या दूरसंचार सेवा को प्रभावित करने वाली किसी सुरक्षा घटना की जानकारी होने के छह घंटे के भीतर प्रभावित प्रणाली के सुसंगत ब्यौरे सहित ऐसी घटना के विवरण सहित इसकी रिपोर्ट केन्द्रीय सरकार को देगी; और

(ख) ऐसी घटना की जानकारी होने के चौबीस घंटे के भीतर, निम्नलिखित जानकारी, जैसा लागू हो, प्रस्तुत करेगी:

(i) सुरक्षा संबंधी घटना से प्रभावित उपयोक्ताओं की संख्या;

(ii) सुरक्षा संबंधी घटना की अवधि;

(iii) सुरक्षा संबंधी घटना से प्रभावित भौगोलिक क्षेत्र;

(iv) दूरसंचार नेटवर्क या दूरसंचार सेवा के कामकाज पर किस हद तक प्रभाव पड़ा है;

(v) किए गए या किए जाने हेतु प्रस्तावित उपचारात्मक उपाय और

(vi) कोई अन्य जानकारी जिसे वह सुसंगत समझता हो।

(2) केन्द्रीय सरकार जहां यह अवधारित करती है कि सुरक्षा घटना का प्रकटन लोकहित में है ऐसी सुरक्षा घटना के बारे में जनता को सूचित कर सकती है या प्रभावित दूरसंचार इकाई को ऐसा करने के लिए आग्रह कर सकती है।

(3) केन्द्रीय सरकार प्रभावित दूरसंचार इकाई से निम्नलिखित उपलब्ध कराने की मांग कर सकती है:

(क) साइबर सुरक्षा उपाय सहित ऐसे दूरसंचार नेटवर्क और दूरसंचार सेवाओं की सुरक्षा का निर्धारण करने के लिए आवश्यक सूचना;

(ख) केंद्रीय सरकार द्वारा यथाअवधारित प्रमाणित अभिकरण द्वारा सुरक्षा संपरीक्षा करना।

(4) केन्द्रीय सरकार किसी सुरक्षा संबंधी घटना के उपचार के लिए या किसी महत्वपूर्ण खतरे की पहचान होने पर उसे घटित होने से रोकने के लिए अपेक्षित उपचारों सहित निदेश जारी कर सकती है तथा प्रभावित दूरसंचार इकाई के लिए ऐसे निदेशों के कार्यान्वयन के लिए समय-सीमा निर्दिष्ट कर सकती है।

8. दूरसंचार पहचानकर्ता और दूरसंचार उपस्कर से संबंधित बाध्यता- (1) उपस्कर का विनिर्माता जिसके पास अंतर्राष्ट्रीय मोबाईल उपस्कर पहचान (आईएमईआई) संख्या है, भारत में निर्मित ऐसे उपस्कर की आईएमईआई संख्या ऐसे उपस्कर के पहले विक्रय से पहले पोर्टल पर ऐसे प्रयोजन के लिए ऐसे प्ररूप में जो केन्द्रीय सरकार द्वारा विनिर्दिष्ट किया जाए, केन्द्रीय सरकार से पंजीकृत कराएगा।

(2) रजिस्ट्रीकृत उपस्कर का आयातक जिसके पास अंतर्राष्ट्रीय मोबाईल उपस्कर पहचान (आईएमईआई) संख्या है, भारत में विक्रय, परीक्षण, अनुसंधान या किसी अन्य प्रयोजन के लिए आयातित ऐसे उपस्कर की आईएमईआई संख्या ऐसे उपस्कर के भारत में आयात से पहले ऐसे प्ररूप में जो पोर्टल पर ऐसे प्रयोजन के लिए विनिर्दिष्ट किया जाए केन्द्रीय सरकार के पास रजिस्ट्रीकृत कराएगा।

(3) कोई भी व्यक्ति-

(क) जानबूझकर विशिष्ट दूरसंचार उपस्कर पहचान संख्या को हटाएगा, मिटाएगा, बदलेगा या परिवर्तित नहीं करेगा; या

(ख) यह जानते हुए कि इसे ऊपर विनिर्दिष्ट अनुसार कॉन्फ़िगर किया गया है, जानबूझकर दूरसंचार पहचानकर्ता या दूरसंचार उपस्कर से संबंधित हार्डवेयर या सॉफ्टवेयर का उपयोग, उत्पादन, यातायात, नियंत्रण या अभिरक्षा अपने पास नहीं रखेगा।

(4) केंद्रीय सरकार छेड़छाड़ किए गए दूरसंचार उपस्कर या अंतर्राष्ट्रीय मोबाईल उपस्कर पहचान (आईएमईआई) संख्या के संबंध में यथाअपेक्षित सहायता प्रदान करने के लिए आईएमईआई संख्या वाले दूरसंचार उपस्कर के निर्माताओं को निदेश जारी कर सकती है।

(5) केंद्रीय सरकार दूरसंचार नेटवर्कों में या दूरसंचार सेवाएं प्रदान करते समय छेड़छाड़ किए गए अंतर्राष्ट्रीय मोबाईल उपस्कर पहचान (आईएमईआई) संख्या वाले दूरसंचार उपस्करों के उपयोग को रोकने के लिए दूरसंचार इकाइयों को निदेश जारी कर सकती है।

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

10. डिजिटल कार्यान्वयन- (1) केंद्रीय सरकार इन नियमों के डिजिटल कार्यान्वयन के प्रयोजन के लिए एक पोर्टल अधिसूचित करेगी तथा कोई अन्य कार्यान्वयन तंत्र भी निर्दिष्ट कर सकती है।

(2) जहां केंद्रीय सरकार दूरसंचार इकाईयों या दूरसंचार उपकरणों के निर्माताओं या आयातकों को कोई आदेश, निदेश या अनुदेश जारी करने के लिए या ऐसी दूरसंचार इकाईयों से कोई सूचना एकत्रित करने के लिए पोर्टल के अलावा संचार के किसी सुरक्षित तरीके का उपयोग करना आवश्यक समझती है, वहां वह संचार के ऐसे सुरक्षित तरीके का उपयोग कर सकेगी।

(3) प्रत्येक दूरसंचार इकाईयों तथा दूरसंचार उपस्कर का विनिर्माता या आयातक, पोर्टल का उपयोग करके या केन्द्रीय सरकार द्वारा यथाअवधारित संचार के सुरक्षित रीति से इन नियमों के अधीन केन्द्रीय सरकार को सूचना देने या प्रस्तुत करने से संबंधित बाध्यताओं का अनुपालन सुनिश्चित करेंगे।

[फा. सं. 24-07/2024-यूबीबी]

देवेंद्र कुमार राय, संयुक्त सचिव

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;

(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.

(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

(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 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 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 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 directions to the telecommunication entity to temporarily suspend use of the relevant telecommunication identifier.

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

(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, 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 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.

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.

(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.

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 manufacturers or importers of telecommunication equipment, or for collection of any information from such telecommunication entities, it may use such secure mode of communication.

(3) Every telecommunication entity 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.