रजिस्ट्री सं० डी० एल०-33004/99

REGD. NO. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

असाधारण
EXTRAORDINARY
भाग II—खण्ड 3—उप-खण्ड (i)
PART II—Section 3—Sub-section (i)
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 15] नई दिल्ली, बृहस्पतिवार, जनवरी 16, 2014/पौष 26,1935
No. 15] NEW DELHI, THURSDAY, JANUARY 16, 2014/PAUSHA 26, 1935

संचार और सूचना प्रौद्योगिकी मंत्रालय
(इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग)
अधिसूचना
नई दिल्ली, 16 जनवरी, 2014

सा. का.नि. 18(अ). – केन्द्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 70 क की उपधारा (1), द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र, ब्लाक-III, जेएनयू कैम्पस, नई दिल्ली 110067, जोकि राष्ट्रीय तकनीकी अनुसंधान संगठन के अंतर्गत एक संगठन है, को महत्वपूर्ण सूचना अवसंरचना संरक्षण के संबंध में राष्ट्रीय नोडल अभिकरण/अभिहित करती है।

[फा. सं. 9(16)/2004-ई.सी.]
आर.के. गोयल, संयुक्त सचिव

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Electronics and Information Technology)

NOTIFICATION

New Delhi, the 16th January, 2014

S.O. 18(E). – In exercise of the powers conferred by sub-section (1) of Section 70A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby designates the National Critical Information Infrastructure Protection Centre, Block-III, JNU Campus, New Delhi-110067, an organisation under the National Technical Research Organisation, as the national nodal agency in respect of Critical Information Infrastructure Protection.

[No. 9(16)/2004-EC]
R.K. GOYAL, Jt. Secy.

अधिसूचना

नई दिल्ली, 16 जनवरी, 2014

सा.का.नि.19(अ).- केन्द्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 70क की उपधारा (3) के साथ पठित धारा 87 की उपधारा (2) के खण्ड (यग) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात:-

1. **संक्षिप्त नाम और प्रारम्भ—** (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र और कार्यों तथा दायित्वों के निर्वहन की रीति) नियम, 2013 है।

(2) ये राजपत्र से उनके प्रकाशन की तारीख से प्रवृत्त होंगे।

2. **परिभाषाएं—** (1) इन नियमों से जब तक अन्यथा संदर्भ अपेक्षित न हो, -

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) "उपयुक्त सरकार" से अधिनियम की धारा 2 की उपधारा (1) के खण्ड (ङ) में परिभाषित अनुसार उपयुक्त सरकार अभिप्रेत है;

(ग) "निगमित निकाय" से अधिनियम की धारा 43क के स्पष्टीकरण (1) में परिभाषित निगमित निकाय अभिप्रेत है;

(घ) "महत्वपूर्ण सूचना अवसंरचना" से अधिनियम की धारा 70 के उपखण्ड के स्पष्टीकरण में परिभाषित महत्वपूर्ण सूचना अवसंरचना अभिप्रेत है;

(ङ) "महत्वपूर्ण सेक्टर" से ऐसे सेक्टर अभिप्रेत हैं, जो राष्ट्र के लिए महत्वपूर्ण हैं और जिनके अक्षम बनाने या विनाश से राष्ट्रीय सुरक्षा, अर्थव्यवस्था, लोक स्वास्थ्य या सुरक्षा पर प्रतिकूल प्रभाव पड़ेगा ;

(च) "भारतीय कम्प्यूटर आपात प्रतिक्रिया दल" से अधिनियम की धारा 70ख की उपधारा (1) के अंतर्गत अधिसूचित भारतीय कम्प्यूटर आपात प्रतिक्रिया दल अभिप्रेत है;

(छ) "मध्यवर्ती" से अधिनियम की धारा 2 की उपधारा (1) के खण्ड (ब) में परिभाषित "मध्यवर्ती" अभिप्रेत है;

(ज) "नोडल अधिकारियों" से समुचित सरकार (सरकारों) और उसके अभिकरणों, निगमित निकायों और महत्वपूर्ण क्षेत्रों में अभिहित निकायों के नामनिर्दिष्ट अधिकारी अभिप्रेत हैं, जो अभिहित नोडल अभिकरण या उसकी इकाइयों को जब भी आवश्यक हो, महत्वपूर्ण सूचना अवसरंचना और संबद्ध संरक्षित प्रणालियों के संरक्षण के लिए सूचित करेंगे, सहयोग देंगे और सहायता प्रदान करेंगे ;

(झ) "तकनीकी केन्द्र" से राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र या उचित सरकारों और इसकी एजेंसियों की तकनीकी इकाइयां अभिप्रेत हैं, जो महत्वपूर्ण सूचना अवसंरचना की संरक्षा के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना के साथ ससंजक और सहयोग से कार्य करेगा।

(2) इन नियमों में प्रयुक्त शब्द और अभिव्यक्ति जो परिभाषित नही हैं परन्तु अधिनियम में परिभाषित है, का वही अर्थ होगा जो अधिनियम में है।

3. (1) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र अधीन अभिहित (इसके पश्चात एनसीआईआईपीसी कहा गया है) महत्वपूर्ण सूचना अवसरंचना के संरक्षण के संबंध में अधिनियम की धारा 70क के अधीन अभिहित राष्ट्रीय नोडल अभिकरण होगा और अधिसूचित किए जाने वाले पते में से कार्य करेगा ।

(2) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र राष्ट्रीय तकनीकी अनुसंधान संगठन (एनटीआरओ) का भाग होगा और एनटीआरओ के प्रशासनिक नियंत्राधीन होगा।

(3) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र सरकारी छुट्टियों सहित वर्ष के सभी दिन चौबीस घंटे कार्य करेगा। एनसीआईआईपीसी का पता और अन्य संपर्क विवरण इसकी वेबसाइट पर प्रकाशित किया जाएगा।

(4) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र का क्षेत्र भारतीय महत्वपूर्ण सूचना अवसंरचना होगा जैसा कि रक्षा मंत्रालय के अधीन अधिसूचित को छोड़कर सरकार द्वारा समय-समय पर अधिसूचित किया जाए।

4. **राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र के कार्य और कर्त्तव्य—** राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र के कार्य और कर्त्तव्य निम्नलिखित होंगे, अर्थात:-

(1) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र राष्ट्र की महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए सभी उपाय करने के लिए राष्ट्रीय नोडल अभिकरण के रूप में कार्य करेगा।

(2) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र साइबर आतंकवाद, साइबर वारफेयर और अन्य खतरों के विरूद्ध महत्वपूर्ण सूचना अवसंरचना की भेद्यता कम करने के उद्देश्य से अनिवार्यत: संरक्षण करेगा और परामर्श देगा।

(3) अधिसूचित करने के लिए उपयुक्त सरकार द्वारा अनुमोदन हेतु सभी महत्वपूर्ण सूचना अवसंरचना घटकों की पहचान करना।

(4) अभिनिर्धारित महत्वपूर्ण सूचना अवसंरचना के विरुद्ध साइबर सुरक्षा खतरों का सामना करने के लिए सरकारों को भी सामरिक नेतृत्व और सामंजस्य प्रदान करना।

(5) पूर्व चेतावनी या सतर्कता के लिए नीति मार्गदर्शन विशेषज्ञता-हिस्सेदारी तथा स्थितिजन्य जागरूकता के लिए महत्वपूर्ण सूचना अवसंरचना को राष्ट्रीय स्तरीय खतरों के समन्वय, भागीदारी, मानीटरी, एकत्रण, विश्लेषण और भविष्यवाणी करना। राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना प्रणाली के संरक्षण का आधारभूत दायित्व उस महत्वपूर्ण सूचना अवसंरचना को चलाने वाले अभिकरण का है।

(6) महत्वपूर्ण सूचना अवसंरचना के संरक्षण की बावत उपयुक्त योजनाएं तैयार करने, मानक अपनाने, सर्वोत्तम पद्धतियों को साझा करने और प्रापण प्रक्रमों के परिमार्जन में सहायता करना।

(7) महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए उनके प्रचार-प्रसार और कार्यान्वयन हेतु संरक्षा रणनीतियों, नीतियां, भेद्यता आकलन और लेखा परीक्षण प्रणालियां और योजनाएं तैयार करना।

(8) महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए अन्तरराष्ट्रीय भागीदारियों के साथ व्यापक सार्वजनिक क्षेत्र के उद्योगों, शैक्षिक संस्थाओं के साथ घनिष्ट रूप से कार्य करने के लिए कौशल विकास करने और उसे समर्थ बनाने के लिए नवीन भावी प्रौद्योगिकी के सृजन, सहयोग करने के लिए अनुसंधान और विकास तथा अन्य कार्यकलाप करना, सहायता अनुदान सहित निधियां प्रदान करना।

(9) महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए प्रशिक्षण और जागरूकता कार्यक्रम तैयार करना अथवा आयोजित करना साथ ही लेखापरीक्षा और प्रमाणन अभिकरणों का विकास और प्रशिक्षण।

(10) महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए राष्ट्रीय और अन्तरराष्ट्रीय सहयोग कार्यनीतियां तैयार करना और उनका निष्पादन करना।

(11) भारतीय कम्प्यूटर आपात प्रतिक्रिया दल और इस क्षेत्र तथा सुसंगत क्षेत्रों में कार्यरत अन्य संगठनों के घनिष्ठ समन्वय में पणधारियों के परामर्श से महत्वपूर्ण सूचना अवसंरचना की सुरक्षा और पद्धतियां, प्रक्रियां, निवारण एवं प्रत्युत्तर से संबंधित दिशानिर्देश, परामर्श और सुमदयता या लेखा-परीक्षा आदि जारी करना।

(12) भारतीय कम्प्यूटर आपात दल तथा क्षेत्र में संबंधित अन्य संगठनों के साथ हमलों तथा अन्य भेद्यताओं से संबंधित साइबर घटनाओं और अन्य सूचना का आदान-प्रदान।

(13) महत्वपूर्ण सूचना अवसंरचना को कोई खतरा होने की स्थिति में राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र सूचना मंगा सकता है और महत्वपूर्ण क्षेत्रों या महत्वपूर्ण सूचना अवसंरचना के संबंध में सूचना देने वाले या सूचना रखने वाले व्यक्तियों को निदेश देगा।

5. कृत्यों और कर्त्तव्यों के निर्वहन की रीति—

(1) (क) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र अनिवार्य रूप से महत्वपूर्ण क्षेत्रों के संबंधित नोडल अधिकारियों, भारतीय कम्प्यूटर आपात प्रतिक्रिया दल और क्षेत्र में तथा सुसंगत क्षेत्रों में कार्यरत अन्य संगठनों के साथ घनिष्ठ सहयोग या समन्वय से अपने कार्यों को करेगा और दायित्वों का निर्वहन करेगा।

(ख) खतरों या भेद्यताओं के विरुद्ध कार्रवाई करने की प्राथमिकता साधारणत: अवरोहण क्रम में प्राथमिकता देने के लिए खतरे के प्रकार, कठोरता, प्रभावित निकाय तथा संसाधनों की उपलब्धता और रीति पर होगी, अर्थात :-

(i) खतरा या भेद्यता से राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना को महत्वपूर्ण भौतिक या आर्थिक या अन्य नुकसान हो सकता है;

(ii) महत्वपूर्ण सूचना अवसंरचना के अधीन शामिल सरकारी संपत्ति को खतरा है;

(iii) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना के पर्याप्त संख्या में क्षेत्र को खतरा है;

(iv) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना का एक विशिष्ट क्षेत्र खतरे में है।

(2) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र के साथ संपर्क

(क) विभिन्न महत्वपूर्ण क्षेत्रों में संबंधित नोडल अधिकारी राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र के साथ संचार के सभी उपयुक्त या उपलब्ध साधनों का प्रयोग करके सम्पर्क करेंगे।

(ख) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र अपने ध्यान में आने वाली किसी भेद्यताओं/खतरे, और जो राष्ट्र की महत्वपूर्ण सूचना अवसंरचना को प्रभावित करते हैं या कर सकते हैं, का स्व: प्रेरणा से संज्ञान लेगा और उपयुक्त उपाय करेगा।

(ग) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र घटनाओं की रिपोर्टिंग के लिए 24X7 हेल्प डेस्क रखेगा।

(3) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र – प्रचालन और अनुक्रिया

(क) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र, संबंधित नोडल अधिकारियों और अन्य अभिकरणों जैसे इस क्षेत्र में कार्यरत कम्प्यूटर आपात प्रतिक्रिया दल के के साथ संयुक्त रूप से सहयोग से परामर्श या चेतावनियां जारी करेगा और महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए खतरे/भेद्यताओं का समाधान करने में मार्गदर्शन और विशेषज्ञता का योगदान करेगा।

(ख) संभावित/वास्तविक राष्ट्र स्तरीय खतरे की दशा में यह निर्णायक भूमिका निभाएगा और महत्वपूर्ण सूचना अवसंरचना के क्षेत्र में भारतीय कम्प्यूटर आपात प्रतिक्रिया दल के घनिष्ठ सहयोग से विभिन्न पणधारियों की प्रतिक्रिया का समन्वय करेगा।

(ग) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना केंद्र, महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए ट्रैफिक डाटा की मानीटरी और संग्रहण के लिए महत्वपूर्ण सूचना अवसंरचना विनिर्दिष्ट और केवल उनकी साइबर संरक्षण आवश्यकताओं से सुसंगत अधिनियम की धारा 69ख और तदधीन अधिसूचित नियमों का आवलंब ले सकेगा।

(घ) महत्वपूर्ण सूचना अवसंरचना के संरक्षण के प्रयोजन के लिए साइबर सूचना के अवरोधन/मानीटरी/उसे डिक्रिप्ट करने तथा ब्लाक करने के लिए राष्ट्रीय महत्वपूर्ण अवसंरचना केंद्र की शक्तियां गृह मंत्रालय तथा एनटीआरओ द्वारा संयुक्त रूप से तैयार कानून और मानक परिचालन प्रक्रियाओं/पद्धतियों के अनुसार होंगी।

6. सलाहकार समिति—

(क) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना केंद्र को अधिदेशित कर्तव्यों और भूमिका को पूरा करने के लिए नीति विषयों और महत्वपूर्ण सूचना अवसंरचना के संरक्षण के से संबंधित उपायों पर परामर्श देने के लिए एक परामर्शदाता समिति होगी।

(ख) सलाहकार समिति का गठन निम्नलिखित से मिलकर होगा :-

(I)	अध्यक्ष/वैज्ञानिक सलाहकार, एनटीआरओ	- अध्यक्ष
(II)	गृह मंत्रालय का प्रतिनिधि	- सदस्य
(III)	विधि एवं न्याय मंत्रालय का प्रतिनिधि	- सदस्य
(IV)	दूर संचार विभाग का प्रतिनिधि	- सदस्य
(V)	इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग का प्रतिनिधि	- सदस्य
(VI)	व्यय विभाग का प्रतिनिधि	- सदस्य
(VII)	रक्षा मंत्रालय का प्रतिनिधि	- सदस्य
(VIII)	महानिदेशक, सर्ट-इन	- सदस्य
(IX)	राष्ट्रीय सुरक्षा परिषद सचिवालय का प्रतिनिधि	- सदस्य
(X)	मंत्रिमंडल सचिवालय का प्रतिनिधि	- सदस्य
(XI)	विषय/डोमेन विशेषज्ञ (अध्यक्ष द्वारा नामानिर्दिष्ट)	- सदस्य
(XII)	एनटीआरओ के दो प्रतिनिधि	- सदस्य
(XIII)	आसूचना ब्यूरो का प्रतिनिधि	- सदस्य
(XIV)	यथाअपेक्षित किसी अन्य मंत्रालय का प्रतिनिधि	- विशेष आमंत्रित
(XV)	(क) उद्योग (ख) निगमित निकाय (ग) महत्वपूर्ण क्षेत्रों के प्रतिनिधि	- विशेष आमंत्रित
(XVI)	राज्य सरकारों के प्रतिनिधि (चक्रानुक्रम के आधार पर)	- विशेष आमंत्रित
(XVII)	महानिदेशक, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र	-सदस्य-संयोजक

(ग) यथाअपेक्षित अनुसार सलाहकार समिति की बैठक होगी।

(घ) एनसीआईआईपीसी के कार्यकरण से संबंधित किसी विशिष्ट मुद्दे का समाधान करने के लिए सलाहकार समिति उप-समितियों का गठन कर सकेगी।

7. अनुसंधान और विकास—

राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र इस संबंध में सरकार के नियमों और प्रक्रियाओं के अनुसार अनुसंधान और विकास में सहयोग (प्रत्यक्ष या अप्रत्यक्ष) के लिए निम्नलिखित से सहयोग की मांग तथा अनुरोध कर सकेगा -

(i) सरकारी संगठन अथवा निकाय, संस्थान, विकास, अभिकरण या सोसायटियां आदि;

(ii) भारत में या भारत से बाहर के विख्यात संस्थान;

(iii) निगमित निकाय तथा उद्योग संघ; तथा

(iv) विषय या डोमेन विशेषज्ञ

[फा. सं. 9(16)/2004-ई.सी.]

आर.के. गोयल, संयुक्त सचिव

NOTIFICATION

New Delhi, the 16th January, 2014

G.S.R. 19(E).- In exercise of the powers conferred by clause (zc) of sub-section (2) of Section 87, read with sub-section (3) of section 70A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:-

1. Short title and Commencement.— (1) These rules may be called the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.

(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 Information Technology Act, 2000 (21 of 2000);

(b) "Appropriate Government" means appropriate Government as defined in clause (e) of sub-section (1) of section 2 of the Act;

(c) "Body Corporate" means body corporate as defined in Explanation (1) to section 43A of the Act;

(d) "Critical Information Infrastructure" means Critical Information Infrastructure as defined in Explanation to sub-section (1) of section 70 of the Act;

(e) "Critical Sector" means sectors, which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health or safety;

(f) "Indian Computer Emergency response Team" means the Indian Computer Emergency Response Team notified under sub-section (1) of section 70B of the Act;

(g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(h) "Nodal Officers" means officer(s) nominated by the appropriate Government(s) and its agencies, body corporates, and other entities in the designated critical sectors, who shall inform, cooperate with and support the designated Nodal Agency or its units as and when required for the protection of Critical Information Infrastructure and associated protected systems;

(i) "Technical Centre" means technical units of the National Critical Information Infrastructure Protection Centre or critical sector(s) or of the appropriate Governments and its agencies, which shall work cohesively in synergistic manner with the National Critical Information Infrastructure Protection Centre for the protection of Critical Information Infrastructure.

(2) Words and expressions used in these rules but not defined and defined in the Act shall have the same meaning as is assigned to them in the Act.

3. (1) National Critical Information Infrastructure Protection Centre (hereinafter referred to as NCIIPC) shall be the national nodal agency designated under section 70A of the Act in respect of Critical Information Infrastructure Protection and shall function at the address to be notified.

(2) National Critical Information Infrastructure Protection Centre shall be a part of and under the administrative control of the National Technical Research Organisation (NTRO),

(3) National Critical Information Infrastructure Protection Centre shall function on a twenty-four-hour basis on all days of the year including Government holidays. The address and other contact details of NCIIPC shall be published on its website.

(4) National Critical Information Infrastructure Protection Centre constituency shall be the Indian critical information infrastructure as notified by the Government from time to time and excluding those notified under the Ministry of Defence.

4. Functions and duties of the National Critical Information Infrastructure Protection Centre.— The functions and duties of the National Critical Information Infrastructure Protection Centre shall be the following, namely:-

(1) National Critical Information Infrastructure Protection Centre shall function as the national nodal agency for all measures to protect nation's critical information infrastructure.

(2) The National Critical Information Infrastructure Protection Centre shall essentially protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats.

(3) Identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.

(4) Provide strategic leadership and coherence across Government to respond to cyber security threats against the identified critical information infrastructure.

(5) Coordinating, sharing, monitoring, collecting, analysing and forecasting, national-level threats to critical information infrastructure for policy guidance, expertise-sharing and situational awareness for early warning or alerts. The basic responsibility for protecting critical information infrastructure system shall lie with the agency running that critical information infrastructure.

(6) Assisting in the development of appropriate plans, adoption of standards, sharing of best practices and refinement of procurement processes in respect of protection of Critical Information Infrastructure.

(7) Evolving protection strategies, policies, vulnerability assessment and auditing methodologies and plans for their dissemination and implementation for protection of Critical Information Infrastructure.

(8) Undertaking research and development and allied activities, providing funding (including grants-in-aid) for creating, collaborating and development of innovative future technology for developing and enabling the growth of skills, working closely with wider public sector industries, academia et al and with international partners for protection of Critical Information Infrastructure.

(9) Developing or organising training and awareness programs as also nurturing and development of audit and certification agencies for protection of Critical Information Infrastructure.

(10) Developing and executing national and international cooperation strategies for protection of Critical Information Infrastructure.

(11) Issuing guidelines, advisories and vulnerability or audit notes etc. relating to protection of critical information infrastructure and practices, procedures, prevention and response in consultation with the stake holders, in close coordination with Indian Computer Emergency Response Team and other organisations working in the field or related fields.

(12) Exchanging cyber incidents and other information relating to attacks and vulnerabilities with Indian Computer Emergency Response Team and other concerned organisations in the field.

(13) In the event of any threat to critical information infrastructure the National Critical Information Infrastructure Protection Centre may call for information and give directions to the critical sectors or persons serving or having a critical impact on Critical Information Infrastructure.

5. Manner of performing functions and duties.—

(1) (a) The National Critical Information Infrastructure Protection Centre shall essentially undertake its task and discharge its responsibilities in close association or coordination with the respective nodal officers of the critical sectors, Indian Computer Emergency Response Team and other organisations working in the field or related fields.

(b) Prioritisation of actions against threats or vulnerabilities shall generally be based on the type, severity, affected entity and availability of resources and the methodology for prioritization in descending order shall be as follows, namely:-

(i) the threat or vulnerability could result in significant physical or economic or other damage to the national critical information infrastructure;

(ii) Government property covered under critical information infrastructure, is in danger;

(iii) a significant number of sector(s) of the national critical information infrastructure are in danger;

(iv) a particular sector of the national critical information infrastructure is endangered.

(2) Communication with National Critical Information Infrastructure Protection Centre

(a) The respective nodal officers in the various critical sectors shall communicate with the National Critical Information Infrastructure Protection Centre using all appropriate or available means of communication.

(b) The National Critical Information Infrastructure Protection Centre may also take suo moto cognizance of any vulnerability/threat that comes to its notice and that affects, or can affect, the nation's Critical Information Infrastructure, and initiate suitable measures.

(c) The National Critical Information Infrastructure Protection Centre shall maintain a 24X7 help desk to facilitate reporting of incidents.

(3) National Critical Information Infrastructure Protection Centre – Operations and Response

(a) National Critical Information Infrastructure Protection Centre shall, in conjunction with the respective nodal officers and other agencies like Indian Computer Emergency Response Team working in the field, issue advisories or alerts and provide guidance and expertise-sharing in addressing the threats/vulnerabilities for protection of Critical Information Infrastructure.

(b) It shall, in the event of a likely/actual national-level threat, play a pivotal role and coordinate the response of the various stake-holders in the area of critical information infrastructure in close cooperation with Indian Computer Emergency Response Team.

(c) For protection of critical information infrastructure, the National Critical Information Infrastructure Protection Centre may take recourse for monitoring and collection of traffic data in accordance with the provisions of section 69B of the Act and the rules notified thereunder specific to critical information infrastructure and relevant to their cyber protection needs only.

(d) The powers to the National Critical Information Infrastructure Protection Centre for interception/monitoring/decryption and blocking of cyber information for the purpose of protection of critical information infrastructure shall be in accordance with the law and as per the Standard Operating Procedures/modalities to be jointly developed by Ministry of Home Affairs and NTRO.

6. **Advisory Committee.—**

(a) There shall be Advisory Committee to advise the National Critical Information Infrastructure Protection Centre on policy matters and measures relating to the protection of critical information infrastructure to enable it to fulfil its mandated role and functions.

(b) The Advisory Committee shall consist of the following:-

(i)	Chairman/Scientific Advisor, NTRO	- Chairman
(ii)	Representative of Ministry of Home Affairs	- Member
(iii)	Representative of Ministry of Law & Justice	- Member
(iv)	Representative of Department of Telecommunications	- Member
(v)	Representative of Department of Electronics & IT	- Member
(vi)	Representative of Department of Expenditure	- Member
(vii)	Representative of Ministry of Defence	- Member
(viii)	Director General, CERT-IN	- Member
(ix)	Representative of National Security Council Secretariat	- Member
(x)	Representative of Cabinet Secretariat	- Member
(xi)	Subject/Domain Experts (Nominated by the Chairman)	- Member(s)
(xii)	Two Representatives from NTRO	- Member(s)
(xiii)	Representative of Intelligence Bureau	- Member
(xiv)	Representative of any other Ministry as and when required	- Special Invitee
(xv)	Representatives from (a) Industry (b) body corporate (c) Critical Sectors	- Special Invitee
(xvi)	Representative of State Governments (by rotation)	- Special Invitee
(xvii)	Director General, National Critical Information Infrastructure Protection Centre	- Member Convener

(c) The Advisory Committee shall meet as often as considered necessary.

(d) The Advisory Committee may constitute Sub-committees to address any specific issue relating to functioning of NCIIPC.

7. **Research and development.—**

The National Critical Information Infrastructure Protection Centre may seek collaboration and support research and development (direct or indirect) in accordance with rules and procedures of Government in this regard from-

(i) Government organisations or bodies, institutes, Departments, agencies or societies etc.;

(ii) institutes of eminence within and/or outside India;

(iii) body corporates and industry associations; and

(iv) subject or domain experts.

[F. No. 9(16)/2004-EC]

R.K. GOYAL, Jt. Secy.

अधिसूचना

नई दिल्ली, 16 जनवरी, 2014

सा.का.नि. 20(अ).- केन्द्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 70ख की उपधारा (5) के साथ पठित धारा 87 की उपधारा (2) के खण्ड (यच) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात:-

1. **संक्षिप्त नाम और प्रारम्भ**— (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (भारतीय कम्प्यूटर आपात प्रतिक्रिया दल और कार्यों और दायित्वों के निर्वहन की रीति) नियम, 2013 है।

(2) ये राजपत्र में उनके प्रकाशन की तारीख से प्रवृत्त होंगे।

2. **परिभाषाएं.**— (1) इन नियमों में जब तक संदर्भ अन्यथा से अपेक्षित न हो, -

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) "कम्प्यूटर संदूषण" से सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 43 (i) में परिभाषित कम्प्यूटर संदूषण अभिप्रेत है;

(ग) "कम्प्यूटर आपात प्रतिक्रिया" से साइबर सुरक्षा आपातकाल के दौरान समन्वय करना, प्रयोक्ताओं को घटना प्रत्युत्तर सेवाएं प्रदान करना, भेद्यताओं और खतरों से संबंधित चेतावनियां प्रकाशित करना और साइबर सुरक्षा में सुधार करने में सहायता के लिए सूचना की प्रस्तावना करना अभिप्रेत है;

(घ) "कम्प्यूटर संसाधन" से सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 2(1) (ट) में परिभाषित कम्प्यूटर संसाधन अभिप्रेत है;

(ङ) "कम्प्यूटर सुरक्षा घटना" से साइबर सुरक्षा घटना अभिप्रेत है;

(च) "साइबर सुरक्षा" से सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 2(1) (ढख) में यथा परिभाषित साइबर सुरक्षा अभिप्रेत है;

(छ) "साइबर घटना" से कोई वास्तविक या संभावित प्रतिकूल घटना अभिप्रेत है जिससे गोपनीयता, सत्यनिष्ठा या इलेक्ट्रॉनिक सूचना प्रणालियों, सेवाओं या नेटवर्क को हानि पहुंचाकर सार्वजनिक तथा निजी क्षेत्रों के महत्वपूर्ण कार्यों तथा सेवाओं के प्रति अपराध या उल्लंघन होने या हानि की संभावना है, जिसके फलस्वरूप अनधिकृत पहुंच, सेवा की मनाही या बाधा, कम्प्यूटर साधन का अनधिकृत उपयोग, प्राधिकार के बिना डेटा या सूचना में परिवर्तन, या सार्वजनिक सुरक्षा को खतरा, जनता के विश्वास को क्षति पहुंचाना, राष्ट्रीय अर्थव्यवस्था पर नकारात्मक प्रभाव या राष्ट्र की सुरक्षा कम होती है;

(ज) "साइबर सुरक्षा घटना" से साइबर सुरक्षा से संबंधित कोई वास्तविक अथवा संभावित प्रतिकूल घटना अभिप्रेत है जिससे अनधिकृत पहुंच, सेवा की मनाही अथवा व्यवधान, सूचना के संसाधन अथवा भण्डारण के लिए किसी कंप्यूटर स्रोत के अनधिकृत प्रयोग अथवा डेटा में परिवर्तन, प्राधिकार के बिना सूचना प्राप्त करने के परिणामस्वरूप लागू सुरक्षा नीति के निहतार्थ अथवा स्पष्ट का उल्लंघन होता है।

(झ) "साइबर सुरक्षा भंग" में किसी व्यक्ति तथा अस्तित्व और अनुरक्षित सत्यनिष्ठा या किसी कंप्यूटर संसाधन में अनुरक्षित सूचना की उपलब्धता का अनधिकृत प्रापण या अनधिकृत उपयोग अभिप्रेत है;

(ञ) "महानिदेशक" से भारतीय कम्प्यूटर आपात प्रतिक्रिया दल का महानिदेशक अभिप्रेत है;

(ट) "भारतीय कम्प्यूटर आपात प्रतिक्रिया दल" से अधिनियम की धारा 70(ख) की उप-धारा (1) के अधीन स्थापित भारतीय कम्प्यूटर आपात प्रतिक्रिया दल अभिप्रेत है;

(ठ) "सूचना" से सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 2(1)(v) में परिभाषित सूचना अभिप्रेत है;

(ड) "सूचना सुरक्षा प्रणालियों" से साइबर सुरक्षा घटनाओं और उल्लंघनाओं को न्यूनतम करने के उद्देश्य से सुरक्षा नीतियों और मानकों का कार्यान्वयन अभिप्रेत है;

(ढ) "राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र " से अधिनियम की धारा 70(ख) की उपधारा (1) के अंतर्गत स्थापित महत्वपूर्ण सूचना अवसंरचना की सुरक्षा के लिए राष्ट्रीय नोडल अभिकरण अभिप्रेत है;

(ण) *"सुरक्षा नीति" से सूचना और कम्प्यूटर संसाधन की सुरक्षा के लिए प्रलेखित व्यवसाय नियम और प्रक्रियाएं अभिप्रेत है;*

(त) "भेद्यता" से किसी कम्प्यूटर सॉफ्टवेयर संसाधन में मौजूद खराबी या हार्डवेयर अथवा सॉफ्टवेयर में त्रुटि अभिप्रेत है जिसका दुरुपयोग किया जा सकता है और फलस्वरूप इंगित कार्यों के बजाए उनके प्रतिकूल या विभिन्न कार्यकरण पर प्रभाव पड़ सकता है ।

(2) इन नियमों में प्रयुक्त शब्द और अभिव्यक्ति जो परिभाषित नही हैं लेकिन जिन्हें अधिनियम में परिभाषित किया गया है, का वही अर्थ होगा जो उनका अधिनियम में है।

3. अवस्थिति— भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (जिसे इसके पश्चात इन नियमों में सर्ट-इन कहा गया है) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग, संचार और सूचना प्रौद्योगिकी मंत्रालय से कार्य करेगा और "इलेक्ट्रॉनिक्स निकेतन", 6, सीजीओ कॉम्प्लेक्स, लोदी रोड़, नई दिल्ली – 110003 में अवस्थित होगा।

4. प्राधिकार— सर्ट-इन इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग, संचार और सूचना प्रौद्योगिकी मंत्रालय का एक अंग होगा और इसके नियंत्राधीन होगा।

5. 24- घंटे आधार पर कार्य करना— सर्ट-इन सरकारी तथा अन्य छुट्टी के दिनों सहित वर्ष के सभी दिनों में 24-घंटे कार्य करेगा और सर्ट-इन का संपर्क विवरण इसकी वेबसाइट www.cert-in.org.in पर प्रकाशित किया जाएगा जिसे समय-समय पर अद्यतन किया जाएगा।

6. सलाहकार समिति— एक सलाहकार समिति सर्ट-इन को साइबर सुरक्षा से संबंधित नीति के मामलों और सेवाओं पर सलाह देगी ताकि यह अधिदेशित भूमिका और कर्त्तव्यों को पूरा करने में समर्थ हो। सलाहकार समिति का गठन निम्नलिखित से मिलकर होगा :

(I)	सचिव, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग	....	अध्यक्ष;
(II)	रक्षा मंत्रालय का प्रतिनिधि	....	सदस्य;
(III)	गृह मंत्रालय का प्रतिनिधि	....	सदस्य;
(IV)	विधि और न्याय मंत्रालय का प्रतिनिधि	....	सदस्य;
(V)	दूर संचार विभाग का प्रतिनिधि	....	सदस्य;
(VI)	राष्ट्रीय सुरक्षा परिषद सचिवालय का प्रतिनिधि	....	सदस्य;
(VII)	राष्ट्रीय महत्वपूर्ण सूचना अवसंचरना संरक्षण केन्द्र का प्रतिनिधि	....	सदस्य;
(VIII)	इंडियन इंस्टीट्यूट ऑफ साइंस बंगलुरू का प्रतिनिधि	....	सदस्य;
(IX)	विभिन्न भारतीय उद्योग संघों से ठीक पूर्ववर्ती वर्ष में परिषद का प्रतिनिधित्व करने वाले उद्योग संघों से पुनर्नियुक्ति के बिना प्रतिवर्ष बारी-बारी से चयनित भारतीय उद्योग संघ का प्रतिनिधि,	....	सदस्य;
(X)	यथाअपेक्षित किसी अन्य मंत्रालय का प्रतिनिधि	....	विशेष आमंत्रित;
(XI)	राज्य सरकारों के प्रतिनिधि (चक्रानुक्रम के आधार पर)	....	विशेष आमंत्रित;
(XII)	महानिदेशक, सर्ट-इन	....	सदस्य संयोजक

7. कार्यक्षेत्र— सर्ट-इन का कार्यक्षेत्र भारतीय साइबर समुदाय होगा।

8. सर्ट-इन के कर्त्तव्य और दायित्व— अधिनियम की धारा 70 ख में यथाविहित के कार्य होंगे। यह साइबर सुरक्षा घटनाओं की अनुक्रिया के लिए भारत में साइबर प्रयोक्ताओं के लिए विश्वस्त अभिकरण और समय-समय पर इसे सौंपे गए कार्य सर्ट-इन पर कार्य करेगा और साइबर सुरक्षा घटनाओं के जोखिम को कम करने के उपाय कार्यान्वित करने में देश में साइबर प्रयोक्ताओं की सहायता करेगा।

9. सेवाएं— सर्ट-इन व्यापक्त: निम्नलिखित सेवाएं प्रदान करेगा:—

- साइबर सुरक्षा घटनाओं पर अनुक्रिया;
- साइबर सुरक्षा घटनाओं की भविष्यवाणी और निवारण;
- साइबर सुरक्षा घटनाओं का विश्लेषण और आपराधिक जांच;
- सूचना सुरक्षा आश्वासन और आडिट;
- साइबर सुरक्षा के क्षेत्र में जागरूकता और प्रौद्योगिकी प्रभावन;
- नियम 10 और नियम 11 के उपनियम (2) के अंतर्गत आने वाले निकायों के लिए तकनीकी जानकारी के लिए प्रशिक्षण अथवा उसका उन्नयन;
- साइबर सुरक्षा में भेद्यताओं के भंग होने पर विद्वेषपूर्ण कार्यकलापों के संबंध में साइबर स्पेस की स्कैनिंग।

186 GI/14-3

10. पणधारी — सर्ट-इन सूचना संग्रहण उसमें भागीदारी और प्रचार-प्रसार और साथ ही साइबर सुरक्षा घटनाओं की अनुक्रिया और निवारण के लिए निम्नलिखित पणधारियों से संपर्क और सहायता प्राप्त करेगा, अर्थात:—

(क) सेक्टोरल कम्प्यूटर आपात प्रतिक्रिया दल;

(ख) मध्यवर्ती;

(ग) इंटरनेट रजिस्ट्री तथा डोमेन रजिस्ट्रार;

(घ) उद्योग;

(ङ) सुरक्षा उत्पादों और सेवाओं सहित सूचना प्रौद्योगिकी उत्पादों के विक्रेता;

(च) शैक्षिक संस्थान, अनुसंधान और विकास संगठन;

(छ) सुरक्षा तथा कानून प्रवर्तन अभिकरण;

(ज) व्यष्टि या व्यष्टियों का समूह;

(झ) अन्तरराष्ट्रीय कम्प्यूटर आपात प्रतिक्रिया दल, मंच और विशेषज्ञ समूह;

(ञ) महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए संलग्न अभिकरण;

(ट) दूरसंचार विभाग।

11. नीतियां और प्रक्रियाएं

(1) घटनाओं की किस्म और सहायता का स्तर—

(क) सर्ट-इन ऐसी सभी साइबर सुरक्षा घटनाओं एवं साइबर घटनाओं का समाधान करेगा जो देश में घटती हों या जिनके घटित होने की संभावना हो लेकिन सर्ट-इन द्वारा दी गई सहायता का स्तर घटना की किस्म तथा गंभीरता, प्रभावित निकाय, व्यष्टि विशेष अथवा व्यष्टियों के समूह, सरकार के संगठन, सार्वजनिक तथा निजी डोमेन और सर्ट-इन के पास उस समय उपलब्ध संसाधन पर अलग-अलग होगा, यद्यपि सभी मामलों में प्रभावित निकाय को और आगे सूचना की किसी क्षति या हानि को न्यूनतम करने के उद्देश्य से यथासंभव कम से कम समय में अनुक्रिया प्रदान की जाएगी। अवरोही क्रम में सूचीबद्ध निम्नलिखित प्राथमिकताओं के अनुसार संसाधन नियमित किए जाएंगे:—

(I) साइबर सुरक्षा घटनाओं और साइबर घटनाओं के कारण मानव की भौतिक सुरक्षा को खतरा;

(II) बैकबोन नेटवर्क अवसंरचना सहित सार्वजनिक सूचना अवसंरचना के भाग में गंभीर प्रकृति की साइबर घटनाएं तथा साइबर सुरक्षा घटनाएं (जैसे सेवा की मनाही, सेवा की वितरित मनाही, घुसपैठ, कम्प्यूटर संदूषण फैलाना);

(III) बड़े-पैमाने पर या बार-बार होने वाली घटनाएं जैसे पहचान चोरी, कम्प्यूटर संसाधन में घुसपैठ, वेबसाइटों को विकृत करना आदि;

(IV) बहुप्रयोक्ता प्रणालियों पर व्यक्ति विशेष के प्रयोक्ता खातों के साथ छेड़-छाड़;

(V) ऊपर वर्णित घटनाओं के अलावा घटनाओं की प्रकृति को उनकी स्पष्ट गंभीरता तथा मात्रा के अनुसार प्राथमिकता दी जाएगी।

(ख) सर्ट-इन साइबर सुरक्षा घटनाओं से उचित रूप से निपटने के लिए प्रभावित निकायों को अनुक्रिया प्रदान करने और सूचना तथा सहायता प्रदान करने का प्रयास करेगा तथा कम्प्यूटर संसाधन की सुरक्षा का अंतिम दायित्व कम्प्यूटर संसाधन के स्वामी का होगा।

(2) सहयोग एवं भागीदारी — सर्ट-इन निम्नलिखित के साथ सहयोग करेगा:—

(I) साइबर सुरक्षा घटनाओं की सुरक्षा और उनकी अनुक्रिया में विशेषज्ञ क्षेत्रों में देश के भीतर तथा देश के बाहर रत संगठन;

(II) साधारणत: कानून प्रवर्तन, जांच और आपराधिक जांच में आसूचना एकत्र करने में लगे संगठन;

(III) शैक्षिक संस्थान, सेवा प्रदाता तथा अनुसंधान और विकास संस्थान;

(IV) व्यक्ति विशेष अथवा व्यक्तियों के समूह।

(3) सर्ट-इन के साथ संपर्क और अधिप्रमाणन— पणधारी और जनता टेलीफोन, फैक्स, ई-मेल, डाक पत्रों जैसे संपर्क साधनों से सर्ट-इन के साथ संपर्क कर सकते हैं। समय-समय पर इसकी वेबसाइट के जरिए उपयुक्त प्रक्रियाओं का प्रचार किया जाएगा।

12. सर्ट-इन के प्रचालन—

(1) घटनाओं की सूचना देना, प्रत्युत्तर और सूचना का प्रचार-प्रसार— साइबर सुरक्षा घटनाओं की सूचना को सुकर बनाने के लिए सर्ट-इन सरकारी और अन्य सार्वजनिक छुट्टियों के दिन सहित सभी दिन में 24 घंटे एक घटना अनुक्रिया हेल्प डेस्क का प्रचालन करेगा।

(क) घटनाओं की सूचना देना: साइबर सुरक्षा घटनाओं द्वारा प्रभावित कोई व्यक्ति विशेष, संगठन या निगमित निकाय घटना की सूचना सर्ट-इन को दे सकता है। अनुबंध में चिह्नित अनुसार साइबर सुरक्षा घटनाओं के प्रकार के बारे में कार्रवाई हेतु यथाशीघ्र सर्ट-इन को रिपोर्ट करना अनिवार्य

होगा। सेवा प्रदाता, मध्यवर्ती डेटा केन्द्र और निगम निकाय घटना होने या ध्यान में आने के यथोचित समय के अन्दर इसकी जानकारी सर्ट-इन को देगा जिससे कि समय से कार्रवाई की जा सके।

साइबर सुरक्षा घटनाओं को सूचित करने की पद्धति और प्रारूप, भेद्यता की सूचना और समाधान, घटना प्रत्युत्तर प्रक्रियाओं और साइबर सुरक्षा संबंधी सूचना के प्रसार के बारे में विवरण सर्ट-इन की वेबसाइट www.cert-in.org.in पर प्रकाशित किया जाएगा और उसे समय-समय पर अद्यतन किया जाएगा।

(2) सर्ट-इन महत्वपूर्ण क्षेत्रों के संबंध में हमलों, भेद्यता तथा समाधान से संबंधित संगत सूचना का राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र के साथ आदान-प्रदान करेगा।

13. सूचना का प्रकटन.—

(1) प्रयोक्ता समुदाय के साथ सम्पर्क और अपने कर्त्तव्यों के निर्वहन के दौरान सर्ट-इन अलग-अलग व्यक्तियों, संगठनों और कम्प्यूटर संसाधन से साइबर सुरक्षा घटनाओं से संबंधित सूचना एकत्र करके उसका विश्लेषण करेगा। सर्ट-इन सूचना के प्रकटन के बारे में सक्षम भारतीय न्यायालयों और लागू नीति-विषयक आदेशों के कानूनी प्रतिबंधों, का पालन करेगा और इस प्रकार की सूचना की गोपनीयता बनाए रखने के लिए यथोचित नियंत्रण बनाए रखेगा और आंतरिक जांच करेगा।

(2) सर्ट-इन भारतीय सक्षम न्यायालयों की स्पष्ट लिखित सहमति या आदेशों के बिना किसी ऐसी सूचना का प्रकटन नहीं करेगा जिससे साइबर घटनाओं और साइबर सुरक्षा द्वारा प्रभावित किसी व्यक्ति, व्यक्तियों के समूह तथा संगठनों की पहचान होती हो। सर्ट-इन सक्षम भारतीय न्यायालयों की स्पष्ट लिखित सहमति या आदेशों के बिना इस प्रकार की सूचना की सुरक्षा के लिए उपयुक्त उपाय करेगा और सूचना में भागीदार व्यक्तियों, व्यक्तियों के समूह तथा संगठनों की पहचान और इसे साइबर सुरक्षा घटनाओं की सूचना का प्रकटन नहीं करेगा।

(3) सर्ट-इन साइबर घटनाओं और साइबर सुरक्षा घटनाओं के समाधान और निवारण तथा जागरूकता को बढ़ावा देने के प्रयोजन से आम जनता की सहायता हेतु सुरक्षा घटनाओं की सामान्य प्रवृत्ति, साइबर सुरक्षा उल्लंघनों के बारे में जानकारी दे सकता है और इनका प्रकटन कर सकता है।

(4) नियम 13 के उपनियम (1), (2) और (3) में यथा उपबंधित के सिवाय सर्ट-इन के लिए भारत की संप्रभुता, भारत की रक्षा, राष्ट्र की सुरक्षा, विदेशों के साथ मित्रता या सार्वजनिक व्यवस्था संज्ञेय अपराध करने के लिए प्रेरित करने से रोकने या देश में साइबर सुरक्षा बढ़ाने के हित में पणधारियों को सभी सुसंगत सूचना का प्रकटन आवश्यक या उचित हो सकता है।

14. अधिनियम की धारा 70 (ख) की उप-धारा (6) के अनुसार सूचना मांगना, कर्त्तव्यों का निर्वहन और अनुपालन—

(1) प्राधिकार—सर्ट-इन का कोई अधिकारी जिसका रैंक भारत सरकार के उप-सचिव के रैंक से अन्यून न हो, अधिनियम की धारा 70(ख) की उपधारा (4) के निर्वहन के लिए सेवा प्रदाताओं, मध्यवर्तियों, डेटा केन्द्रों, निगमित निकायों तथा किसी अन्य व्यक्ति से सूचना मांग सकेगा।

(2) सर्ट-इन, सूचना प्रौद्योगिकी अधिनियम, 2000 और तदधीन अधिसूचित नियमों का साइबर सुरक्षा के लिए ट्रैफिक डाटा की मानीटरी और संग्रहण का अवलम्ब ले सकेगा।

(3) सूचना प्रस्तुत करने के लिए प्रपत्र- सर्ट-इन द्वारा मांगी गयी सूचना निर्धारित अवधि में और सूचना प्रस्तुत करने के लिए भेजे गए पत्र के साथ संलग्न प्रपत्र में प्रस्तुत की जाएगी।

(4) सूचना मांगने एवं सूचना प्रस्तुत करने का ढंग —सर्ट-इन अंकीय रूप से हस्ताक्षरित ई-मेल, फैक्स या पंजीकृत डाक द्वारा सूचना मांग सकेगा। सूचना सर्ट-इन को किसी उपयुक्त संचार माध्यम जैसे अंकीय रूप से हस्ताक्षरित ई-मेल, फैक्स, पंजीकृत डाक पत्रों, रीड केवल काम्पेक्ट डिस्क या रीड केवल डिजिटल वर्सेटाइल डिस्क, सर्ट-इन द्वारा निर्दिष्ट किए अनुसार मात्रा पर निर्भरता के आधार पर प्रस्तुत की जाएगी। जैसा कि नियम 17 में परिभाषित किया गया है, सर्ट-इन इनसे सम्पर्क करने के लिए अपने सर्वर पर एक सुरक्षित अपलोड सुविधा प्रदान कर सकता है।

15. अनुपालन के लिए निदेश— अधिनियम की धारा 70(ख) की उपधारा (6) में भी यथा प्रदत्त अनुसार इसकी अधिदेशित भूमिका और कर्त्तव्यों के अनुसरण में और देश में सूचना अवसंरचना की साइबर सुरक्षा बढ़ाने के उद्देश्य से महानिदेशक, सर्ट-इन सेवा प्रदाताओं, मध्यवर्तियों, डेटा केन्द्रों, निगमित निकाय तथा किसी अन्य व्यक्ति को निदेश या परामर्श जारी करने के लिए किसी अधिकारी का नाम निर्दिष्ट कर सकेगा जिसका रैंक भारत सरकार के निदेशक से नीचे स्तर का न हो। अनुपालन के लिए ऐसे निदेश या परामर्श इलेक्ट्रॉनिक हस्ताक्षरयुक्त ई-मेल, फैक्स या पंजीकृत डाक से जारी किए जाएंगे। सेवा प्रदाता, मध्यवर्ती, डेटा केन्द्र, निगमित निकाय तथा कोई अन्य व्यक्ति इस प्रकार के अनुदेशों या परामर्शों का पालन करेगा और निदेश या परामर्श के अनुसार निर्धारित समय में तथा रीति से सर्ट-इन को सूचित करेगा।

16. अननुपालन रिपोर्ट— समय अवधि के अंतर्गत ऐसे किसी सेवा प्रदाताओं, मध्यवर्तियों, डेटा केन्द्रों, निगमित निकाय और अन्य किसी व्यक्ति के द्वारा समयावधि के अंदर निदेशों के किसी भी अननुपालन के मामले में संबंधी उपर्युक्त अधिकारी ऐसे निदेशों की समाप्ति की तिथि से 2 दिनों के भीतर ऐसे अननुपालन की जानकारी देते हुए महानिदेशक को अननुपालन रिपोर्ट प्रस्तुत करेगा।

17. संपर्क बिंदु— सर्ट- इन के साथ संपर्क करने के लिए सेवा प्रदाता, मध्यवर्ती, डेटा केंद्र और निगमित निकाय एक संपर्क बिंदु निर्धारित करेंगे। संपर्क बिंदु से संबंधित सूचना सर्ट-इन को, सर्ट-इन द्वारा निर्धारित किए गए प्रारूप में भेजी जाएगी और समय-समय पर उसे उद्यतन किया जाएगा। सूचना प्राप्त करने और उसके अनुपालन हेतु निदेश प्राप्त करने के लिए सर्ट-इन से सभी प्रकार का पत्राचार उसी संपर्क बिंदु के साथ किया जाएगा।

18. अननुपालन से निपटना — नियम 14 के अधीन जानकारी प्राप्त करने के लिए किए गए पत्राचार के संबंध में अननुपालन के सभी मामले और नियम 15 के अंतर्गत अननुपालन के लिए जारी निर्देश नियम 19 के अंतर्गत गठित पुनर्विलोकन समिति को प्रस्तुत किए जाएंगे।.

19. पुनर्विलोकन समिति —

(1) निम्नलिखित का पुनर्विलोकन करने के लिए केंद्र सरकार द्वारा एक पुनर्विलोकन समिति गठित की जाएगी -

(क) नियम 14 के अधीन जानकारी प्राप्त करने के लिए सेवा प्रदाताओं, मध्यवर्तियों, डेटा केंद्रों, निगमित निकायों और अन्य किसी व्यक्ति के पत्राचार का अननुपालन;

(ख) नियम 15; के अंतर्गत सेवा प्रदाताओं, मध्यवर्तियों, डेटा केन्द्रों, निगम निकाय और अन्य किसी व्यक्ति को जारी निदेशों का अननुपालन;

(ग) ऐसे नाम निर्दिष्ट सेवा प्रदाताओं, मध्यवर्तियों, डेटा केंद्रों, निगमित निकाय और किसी अन्य व्यक्ति द्वारा नियम 15 के अधीन विनिर्दिष्ट समयावधि के भीतर निदेशों का अननुपालन अधिनियम की धारा 70ख की उपधारा (7) के अंतर्गत अपराध माना जाएगा।

(2) पुनर्विलोकन समिति निम्नलिखित से मिलकर बनेगी:—

(I)	सचिव, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग	.... अध्यक्ष;
(II)	संयुक्त सचिव, विधि और न्याय मंत्रालय	.... सदस्य;
(III)	संयुक्त सचिव स्तर का कोई अधिकारी, दूरसंचार विभाग	....सदस्य;
(IV)	संयुक्त सचिव, गृह मंत्रालय	.... सदस्य;
(V)	समूह प्रमुख (साइबर कानून और ई-सुरक्षा), इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग	.... सदस्य- संयोजक

पुनर्विलोकन समिति की बैठक आवश्यकतानुसार आयोजित होगी।

20. निदेशों के अननुपालन के लिए कार्रवाई— नियम 16 के अधीन पूर्वोक्त संबंधित अधिकारी द्वारा प्रस्तुत अननुपालन रिपोर्ट के आधार पर नियम 19 के अधीन पुनर्विलोकन समिति के ऐसे निदेश के आधार पर महानिदेशक, सर्ट-इन को अधिनियम की धारा 70 (ख) की उपधारा (8) से यथाउपबंधित अनुसार न्यायालय के समक्ष शिकायत करने के लिए किसी अधिकारी को प्राधिकृत करेगा।

[फा. सं. 9(16)/2004-ई.सी.]
आर.के. गोयल, संयुक्त सचिव

NOTIFICATION

New Delhi, the 16th January, 2014

G.S.R 20(E).- In exercise of the powers conferred by clause (zf) of sub-section (2) of section 87, read with sub-section (5) of section 70B of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely :—

1. **Short title and commencement.—** (1) These Rules may be called the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

(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 Information Technology Act, 2000 (21 of 2000);

(b) "Computer contaminant" means computer contaminant as defined in section 43 (i) of the Information Technology Act, 2000;

(c) "Computer emergency response" means to coordinate action during cyber security emergencies, provide incident response services to users, publish alerts concerning vulnerabilities and threats, and offer information to help improve cyber security

(d) "Computer resource" means computer resource as defined in section 2(1)(k) of the Information Technology Act, 2000;

(e) "Computer security incident" means cyber security incident;

(f) "Cyber security" means cyber security as defined in section 2(1)(nb) of the Information Technology Act, 2000;

(g) "Cyber incident" means any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing

the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation;

(h) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(i) "Cyber security breaches" means unauthorised acquisition or unauthorised use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

(j) "Director General" means the Director General of the Indian Computer Emergency Response Team;

(k) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team set up under sub-section (1) of section 70(B) of the Act;

(l) "Information" means information as defined in section 2(1)(v) of the Information Technology Act, 2000;

(m) "Information security practices" means implementation of security policies and standards in order to minimise the cyber security incidents and breaches;

(n) "National Critical Information Infrastructure Protection Centre" means the national nodal agency for protection of Critical Information Infrastructure set up under sub- section (1) of Section 70(B) of the Act;

(o) "Security policy" means documented business rules and processes for protecting information and the computer resource;

(p) "Vulnerability" means the existence of a flaw or weakness in hardware or software of a computer resource that can be exploited resulting in their adverse or different functioning other than the intended functions.

(2) Words and expressions used in these rules but not defined and defined in the Act shall have the same meaning as is assigned to them in the Act.

3. **Location.**— The Indian Computer Emergency Response Team (hereinafter referred in these Rules as CERT-In) shall function at Department of Electronics and Information Technology, Ministry of Communications and Information Technology and shall be located at "Electronics Niketan", 6, CGO Complex, Lodhi Road, New Delhi – 110003.

4. Authority.— CERT-In shall be a part and under the administrative control of the Department of Electronics and Information Technology, Ministry of Communications and Information Technology.

5. **Functioning on 24-hour basis.**— CERT-In shall function on 24-hours basis on all days of the year including Government and other holidays and the contact details of CERT-In shall be published on its website **www.cert-in.org.in** and are updated from time to time.

6. **Advisory Committee.**— An Advisory Committee shall advise CERT-In on policy matters and services related to cyber security to enable it to fulfill its mandated roles and functions. The Advisory Committee shall have the following composition:

(i)	Secretary, Department of Electronics and Information Technology	...Chairman;
(ii)	Representative from the Ministry of Defence	...Member;
(iii)	Representative of the Ministry of Home Affairs	... Member;
(iv)	Representative of the Ministry of Law and justice	....Member;
(v)	Representative of the Department of Telecommunications	....Member;
(vi)	Representative of the National Security Council Secretariat	....Member;
(vii)	Representative of National Critical Information Infrastructure Protection Centre	... Member;
(viii)	Representative of Indian Institute of Science (IISc), Bengaluru	.... Member;
(ix)	Representative of an Indian Industry Association, selected by yearly rotation amongst different Indian Industry Associations, without reappointment from	

the same Industry Association having a representative on the Council in the immediately preceding year ....Member;

(x) Representative of any other Ministry as and when required ...Special Invitee;

(xi) Representative of State Governments (by rotation) ... Special Invitee;

(xii) Director General, CERT-In ....Member Convener.

7. Constituency.— CERT-In constituency shall be the Indian cyber community.

8. Functions and responsibilities of CERT-In.— CERT-In shall have functions as prescribed in section 70B of the Act and those which may be assigned to it from time to time. It shall function as the trusted referral agency for cyber users in India for responding to cyber security incidents and will assist cyber users in the country in implementing measures to reduce the risk of cyber security incidents.

9. Services.— CERT-In shall broadly provide following services:—

- response to cyber security incidents;
- prediction and prevention of cyber security incidents;
- analysis and forensics of cyber security incidents;
- information security assurance and audits;
- awareness and technology exposition in the area of cyber security;
- training or upgrade of technical know-how for the entities covered under Rule 10 and sub-rule(2) of Rule11;
- scanning of cyber space with respect to cyber security vulnerabilities, breaches and malicious activities.

10. Stakeholders.— CERT-In shall interact with and seek assistance from the following stakeholders to collect, share and disseminate information and also to respond and prevent cyber security incidents, namely: :—

(a) Sectoral Computer Emergency Response Teams;

(b) Intermediaries;

(c) Internet Registry and Domain Registrars;

(d) Industry;

(e) Vendors of Information Technology products including security products and services;

(f) Academia, Research and Development Organizations;

(g) Security and Law Enforcement Agencies;

(h) Individuals or group of individuals;

(i) International Computer Emergency Response Teams, Forums and expert groups;

(j) Agency engaged for the protection of Critical Information Infrastructure;

(k) Department of Telecommunications.

11. Policies and procedures.—

(1) **Types of incidents and level of support.—**

(a) CERT-In shall address all types of cyber security incidents cyber incidents which occur or are expected to occur in the country but the level of support given by CERT-In will vary depending on the type and severity of the incident, affected entity, be it individual or group of individuals, organisations in the Government, public and private domain, and the resources available with CERT-In at that time, though in all cases a quick response with an aim to minimize any further damage or loss of information to the affected entity will be made in a shortest possible time. Resources will be assigned according to the following priorities listed in decreasing order:—

(I) threats to the physical safety of human beings due to cyber security incidents;

(II) cyber incidents and cyber security incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant,) on any part of the public information infrastructure including backbone network infrastructure;

(III) large-scale or most frequent incidents such as identity theft, intrusion into computer resource, defacement of websites etc.;

(IV) compromise of individual user accounts on multi-user systems;

(V) types of incidents other than those mentioned above will be prioritised according to their apparent severity and extent.

(b) CERT-In shall endeavour to respond and present information and assistance to the affected entities to deal with cyber security incidents as appropriate and the ultimate responsibility of the security of the computer resource shall rest with owner of the computer resource.

(2) **Cooperation and collaboration.**— CERT-In shall collaborate with:—

(I) organisations within and outside the country engaged in the specialised areas in protecting and responding to cyber security incidents;

(II) organisations engaged in collection of intelligence in general, law enforcement, investigation and forensics;

(III) academia, industry, service providers and research and development institutions;

(IV) individuals or group of individuals.

(3) **Communication and authentication with CERT-In.**— The stakeholders and public at large can communicate with the CERT-In through communication systems ranging from telephone, fax, email and postal letters. The appropriate procedures will be disseminated through its website from time to time.

12. CERT-In operations.—

(1) **Incident reporting, response and Information dissemination.**— CERT-In shall operate an Incident Response Help Desk on 24 hours basis on all days including Government and other public holidays to facilitate reporting of cyber security incidents.

(a) Reporting of incidents: Any individual, organisation or corporate entity affected by cyber security incidents may report the incident to CERT-In. The type of cyber security incidents as identified in Annexure shall be mandatorily reported to CERT-In as early as possible to leave scope for action. Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action.

The details regarding methods and formats for reporting cyber security incidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cyber security shall be published on the website of CERT-In **www.cert-in.org.in** and will be updated from time to time.

(2) CERT-In shall exchange relevant information relating to attacks, vulnerabilities and solutions in respect of critical sector with National Critical Information Infrastructure Protection Centre.

13. Disclosure of information.—

(1) During the course of interaction with user community and discharging its functions CERT-In may collect and analyse information relating to cyber security incidents from individuals, organisations and computer resource. CERT-In shall follow applicable legal restrictions, orders of competent Indian courts and ethical practices with regard to disclosure of information and shall maintain reasonable controls and internal checks to maintain confidentiality of such information.

(2) CERT-In shall not disclose any information which may lead to identification of individual, group of individuals or organizations affected by cyber security incidents without their explicit written consent or orders of Indian competent courts. CERT-In shall take appropriate measures to protect such information and shall also not disclose the identity of individuals, group of individuals and organisations sharing the information and reporting cyber security incidents to it, without their explicit written consent or orders of Indian competent courts.

(3) CERT-In may share or disclose the general trends of cyber security incidents, cyber security breaches freely to assist general public for the purpose of resolving and preventing cyber security incidents and promoting awareness.

(4) Save as provided in sub-rules (1), (2) and (3) of Rule 13, it may be necessary or expedient so to do, for CERT-In to disclose all relevant information to the stakeholders, in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence relating to cognizable offences or enhancing cyber security in the country.

14. Seeking information, carrying out functions and for compliance in terms of sub-section (6) of section 70 (B) of the Act.—

(1) **Authority.**— Any officer of CERT-In, not below the rank of Deputy Secretary to the Government of India may seek information from service providers, intermediaries, data centres, body corporate and any other person for carrying out the functions provided in sub-section (4) of section 70(B) of the Act.

(2) For cyber security, CERT-In may take recourse for monitoring and collection of traffic data in accordance with the provisions of section 69B of the Information Technology Act, 2000 and Rules notified thereunder.

(3) **Format for submission of information.**— The information sought by CERT-In shall be submitted within the duration and in the format provided alongwith the communication sent for seeking the information.

(4) **Manner of seeking and submission of information.**— CERT-In may seek the information through digitally signed email, fax or registered postal mail. The information shall be submitted to CERT-In through any suitable

communication channel such as digitally signed email, fax, registered postal letters, Read only Compact Disc or Read only Digital Versatile Disc, depending upon the volume of information and as specified by CERT-In. CERT-In may also provide a secure upload facility on their server to the individual Point of Contact as defined in Rule 17.

15. Directions for compliance.— In pursuance of its mandated roles and functions as provided in sub-section(4) of section 70(B) of the Act and with a view to enhancing cyber security of the information infrastructure in the country, Director General, CERT-In shall designate, an officer not below the rank of Director to the Government of India, to issue directions or advisory to service providers, intermediaries, data centres, body corporate and any other person. Such directions or advisory for compliance shall be issued by email signed with electronic signature, fax or registered postal mail. The service providers, intermediaries, data centres, body corporate and any other person shall comply with such directions or advisories and also report to CERT-In, within the time period and the manner as provided in the direction or advisory.

16. Report of non-compliance.— In case of any non-compliance of directions within the time period by any such named service providers, intermediaries, data centres, body corporate and any other person, the concerned aforesaid officer shall submit a non-compliance report to the Director General providing details of such non-compliance within two days from the date of expiry of such directions.

17. Point of Contact.— The service providers, intermediaries, data centres and body corporate shall designate a Point of Contact to interface with CERT-In. The information relating to a Point of Contact shall be sent to CERT-In in the format specified by it and shall be updated from time to time. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the said Point of Contact.

18. Dealing with non-compliance.— All cases of non-compliance with respect to the communications seeking information under Rule 14 and directions issued for compliance under Rule 15 shall be submitted to the Review Committee constituted under Rule 19.

19. Review Committee.—

(1) A Review Committee shall be constituted by the Central Government to review the —

(a) non-compliance of the communication, seeking information under Rule 14, issued to the service providers, intermediaries, data centres, body corporate and any other person;

(b) non-compliance of the directions issued to the service providers, intermediaries, data centres, body corporate and any other person under Rule 15;

(c) terming non-compliance of directions within the time period specified under Rule 15 by any such named service providers, intermediaries, data centres, body corporate and any other person as an offence under sub-section (7) of section 70B of the Act.

(2) The Review Committee shall consist of the following:—

(I)	Secretary, Department of Electronics and Information Technology	....	Chairman;
(II)	Joint Secretary, Ministry of Law and Justice	....	Member;
(III)	Joint Secretary Level Officer, Department of Telecommunications	....	Member;
(IV)	Joint Secretary, Ministry of Home Affairs	....	Member;
(V)	Group Coordinator (Cyber Law and e-Security), Department of Electronics & Information Technology	...	Member-Convenor

The Review Committee shall meet as often as necessary.

20. Action for non-compliance of direction.— Based on the non-compliance report as submitted by the concerned aforesaid officer under Rule 16 and such direction of the Review Committee under Rule 19, the Director General shall authorise an officer of CERT-In to file a complaint before the court as provided under sub-section (8) section 70B of the Act

[F. No. 9(16)/2004-EC]

R.K. GOYAL, Jt. Secy.

Printed by the Manager, Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.