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 रोड, 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 अवसंरचना 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।

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 परामर्शो 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 अनुपालन 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