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;*