OFFICE OF THE DIRECTOR
ALL INDIA INSTITUTE OF MEDICAL SCIENCES
Ansari Nagar, New Delhi-110029

F. No.40-30/2023-Estt.-I(DO) Dated: 25th January, 2024

OFFICE MEMORANDUM

Subject: Constitution of Information Security Steering Committee (ISSC) for Critical Information Infrastructure.

The committee "Information Security Steering Committee for Protected Systems and for implementation of Cyber Security Systems at AIIMS, New Delhi" constituted vide OM F.No.40-30/2022-Estt-I(DO) dated 03 November 2023 is hereby dissolved.

Whereas, the central government has declared the computer resources relating to HMIS (Hospital Management Information System), LMIS (Laboratory Management Information System), PACS (Picture Archiving and Communication System) and BBMS (Blood Bank Management System) being Critical Information Infrastructure (CII) of the AIIMS, New Delhi, and the computer resources of its associated dependencies, to be Protected Systems for the purpose of the Information Technology Act, 2000 and authorized certain persons to access the Protected Systems vide its gazette: extraordinary CG-DL-E-27072023-247654 Part-II Section-III-Sub-Section (ii) dated 27 July 2023 (copy attached): AND

Whereas, Rule No. 3(1) of the rules framed under the sub-section (2) of section 87 read with section 70 of the Information Technology Act, 2000 (21 of 2000), published vide gazette notification PART II—Section 3—Sub-section (ii) dated 22 May 2018 provides for constitution of Information Security Steering Committee (ISSC) [copy attached]

In compliance to the same, "**Information Security Steering Committee (ISSC)**" shall have the following roles and responsibilities under Rule No. 3(2) of the said Rules:

a) All the Information Security Policies of the "Protected Systems" shall be approved by the ISSC.
b) Significant changes in the network configuration impacting "Protected Systems" shall be approved by the ISSC.
c) Each significant change in application(s) of the "Protected System" shall be approved by the ISSC.
d) A mechanism shall be established for timely communication of cyber incident(s) related to "Protected System" to ISSC
e) A mechanism shall be established to share the results of all information security audits and compliance of "Protected System" to ISSC.
f) Assessment for validation of "Protected System" after every two years.

The **Information Security Steering Committee (ISSC)** with the following composition is being constituted for the roles and responsibilities mentioned above:

1. Additional Director (Administration), AIIMS – Chairperson
2. Medical Superintendent, AIIMS
3. Dr. Vivek Gupta, Interim Chief Information Security Officer (CISO)
4. Sr. Financial Advisor, AIIMS
5. Representative of NCIIPC
6. Dr Pooja Gupta, PIC-CF
7. Dr. Sudip K Datta, Addl. Professor, Dept. of Laboratory Medicine
8. Mr. Rajiv Gupta, Consultant Cyber Security
9. Dr. Samarth Mittal, Associate Professor of Orthopaedics, JPNATC
10. Dr. Arun Verma, Assistant Professor, Hospital Administration
11. Dr. Devasenathipathy K, Addl. Prof., Radiodiagnosis
12. Mr. Lalit Bhatia, Technical Director, NIC
13. Mr. Shyamal Barua, Sr. Programmer, Computer Facility
14. Mrs. Tripta, Sr. Programmer, Computer Facility
15. Dr. Poonam Coshic, Main Blood Bank, AIIMS
16. Mr. Amit Bhati, Sr. Programmer, Computer Facility – Member Secretary

25/1/2024

(Prof. M. Srinivas)
Director

Distribution: *(with a request to also circulate it to all officials under their control)*

1. Dean(s) (Academic, Research, Examination)
2. Medical Superintendent (AIIMS)
3. Chiefs of all Centres / Head, NCI Jhajjar
4. Heads of all departments
5. All members of the committee
6. Prof. Incharge, CF – With a request to upload this on Institute's website

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 (ii)
PART II—Section 3—Sub-section (ii)
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 2017] नई दिल्ली, शुक्रवार, जून 1, 2018/ज्येष्ठ 11, 1940
No. 2017] NEW DELHI, FRIDAY, JUNE 1, 2018/JYAISTHA 11, 1940

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय

अधिसूचना

नई दिल्ली, 22 मई, 2018

का.आ. 2235(अ).— केंद्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 70 के साथ पठित धारा 87 की उप-धारा (2) के खंड (यख) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए इसके द्वारा निम्नलिखित नियम बनाती है, अर्थात् .—

1. संक्षिप्त नाम और प्रारंभ - (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (संरक्षित प्रणाली के लिए सूचना सुरक्षा प्रथा और प्रक्रिया) नियम, 2018 है।

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

2. परिभाषायें – (1) इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो –

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

(ख) "मुख्य सूचना सुरक्षा अधिकारी" से अभिप्रेत है, वरिष्ठ प्रबंधन के अभिहित कर्मचारी जो संगठन के प्रबंध निदेशक / कार्यपालक अधिकारी / सचिव के संगठन कार्यरत हों और सूचना सुरक्षा और संबंधित मुद्दों का ज्ञान रखते हों, सूचना सुरक्षा नीतियों के नियोजन, विकास, रखरखाव, पुनर्विलोकन और कार्यान्वयन सहित साइबर सुरक्षा प्रयासों और पहलों के लिए जिम्मेदार जिम्मेदार हों;

(ग) "विवेचित सूचना अवसंरचना" से अभिप्रेत है वह अधिनियम की धारा 70 की उप-धारा (1) के विवरण में निर्दिष्ट महत्वपूर्ण सूचना अवसंरचना है;

(घ) "साइबर संकट प्रबंधन योजना" तीव्रता से पहचान, सूचना आदान-प्रदान, तीव्र प्रत्युत्तर और महत्वपूर्ण प्रक्रियाओं को प्रभावित करने वाले दुर्भावनापूर्ण साइबर से संबंधित घटनाओं को कम करने और ठीक करने की उपचारात्मक कार्रवाई के लिए

एक समन्वित, बहु-विषयक और व्यापक आधारित दृष्टिकोण के लिए साइबर संबंधित घटनाओं से निपटने के लिए एक ढांचे की रूपरेखा तैयार करता है;

(ड) "साइबर घटना" से अभिप्राय किसी वास्तविक या संदिग्ध प्रतिकूल घटना से है जो किसी अपराध या उल्लंघन का कारण बनती है या बन सकती है, इलेक्ट्रॉनिक सूचना, तंत्र, सेवाओं या संजाल की गोपनीयता, अखंडता, या उपलब्धता को कम करके सार्वजनिक और प्राइवेट क्षेत्रों में महत्वपूर्ण कार्यों और सेवाओं को नुकसान पहुँचाती हो या पहुँचा सकती है जिसके परिणामस्वरूप अनधिकृत पहुंच, सेवा की मनाई या व्यवधान, किसी कंप्यूटर संसाधन का अनधिकृत उपयोग, डाटा या सूचना में अनधिकृत परिवर्तन होता है; या जो सार्वजनिक स्वास्थ्य या सुरक्षा के लिए खतरा हो, सार्वजनिक विश्वास को कमजोर करती हो, राष्ट्रीय अर्थव्यवस्था पर नकारात्मक प्रभाव डालती हो, या राष्ट्र की सुरक्षा स्थिति को कम करती हो;

(च) "सूचना सुरक्षा प्रबंधन योजना" से अभिप्रेत है नीतियों, प्रक्रियाओं और कार्यप्रणालियों का एक समुच्चय जो कि सूचना सुरक्षा को स्थापित करता है, कार्यान्वित करता है, संचालित करता है, निगरानी करता है, समीक्षा करता है, रखरखाव करता है और लगातार सुधार करता है और पर्याप्त एवं उपयुक्त सुरक्षा नियंत्रणों के विकास, रखरखाव, क्रियान्वयन और समीक्षा से जोखिमों को कम करता है;

(छ) "सूचना सुरक्षा परिचालन समिति" का अभिप्राय है एक ऐसी समिति जिसमें संगठन के उच्च प्रबंधन अधिकारी शामिल हों, जो संरक्षित प्रणाली की साइबर सुरक्षा की स्थिति को लगातार सुधार और मजबूत करने के लिए जिम्मेदार हो और दुर्भावनापूर्ण साइबर घटनाओं को कम करने और उन्हें पुनर्जीवित करने के लिए उपचारात्मक कार्यों की योजना बनाती हो, उनका विकास करती हो और उनकी समीक्षा भी करती हो;

(ज) "सूचना प्रौद्योगिकी सुरक्षा सेवा स्तर करार" से अभिप्रेत है वह सेवा प्रदाताओं और "संरक्षित प्रणाली" से संबंधित सूचना को संरक्षित करने के लिए "संरक्षित प्रणाली" से संबंधित अधिकारियों के बीच विधिक रूप से मान्यता प्राप्त सेवा स्तर करारें;

(झ) "राष्ट्रीय विवेचित सूचना अवसंरचना संरक्षण केंद्र" से अभिप्रेत है वह अधिनियम की धारा 70क की उप-धारा (1) के तहत स्थापित अभिकरण है;

(ञ) "संगठन" से अभिप्रेत है-

(i) भारत सरकार के मंत्रालय या विभाग, राज्य सरकारें और केंद्र शासित प्रदेश;

(ii) केंद्र सरकार, राज्य सरकार और केंद्र शासित प्रदेशों की कोई संस्था;

(iii) कोई अन्य इकाई जिसके पास 'संरक्षित प्रणाली' हो;

(ट) "संरक्षित प्रणाली" से अभिप्रेत है कि वह कोई भी संगठन का कोई भी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर संजाल, जो कि अधिनियम की धारा 70 के अधीन समुचित सरकार द्वारा राजपत्र में अधिसूचित किया गया हो;

(ठ) "सेवा प्रदाता" से अभिप्रेत है प्राधिकृत व्यष्टिक (व्यष्टि को), सरकारी संगठन, पब्लिक सेक्टर की इकाइयां (पीएसयू), प्राइवेट अभिकरण, प्राइवेट कंपनी, भागीदार फर्म या कोई अन्य निकाय या अभिकरण कि "संरक्षित प्रणाली" के निर्बाध और निरंतर कृत्यकारी के लिए सेवाएं प्रदान कर रही हो;

(2) अन्य सभी प्रयुक्त शब्द और अभिव्यक्तियाँ जो कि इन नियमों में परिभाषित नहीं है किंतु अधिनियम में परिभाषित हैं उनका अर्थ वही होगा जो अधिनियम में उनको क्रमशः समनुदेशित है।

3. "संरक्षित प्रणाली" के लिए सूचना सुरक्षा प्रथायें और प्रक्रियायें:

(1) (क) "संरक्षित प्रणाली" रखने वाला संगठन, संगठन के मुख्य कार्यपालक अधिकारी / प्रबंध निदेशक / सचिव के अध्यक्षता में एक सूचना सुरक्षा परिचालन समिति का गठन करेगा।

(ख) सूचना सुरक्षा परिचालन समिति की संरचना निम्नानुसार होगी:

(i) सूचना प्रौद्योगिकी प्रमुख या समकक्ष;

(ii) मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ);

(iii) वित्तीय सलाहकार या समकक्ष;

(iv) राष्ट्रीय विवेचित सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) का प्रतिनिधि;

(v) संगठन द्वारा नामनिर्दिष्ट अन्य विशेषज्ञ (एक या एक से अधिक);

(2) सूचना सुरक्षा परिचालन समिति (आईएसएससी) निम्न भूमिकाओं और उत्तरदायित्वों के साथ शीर्ष निकाय होगा: -

(क) "संरक्षित प्रणाली" की सभी सूचना सुरक्षा नीतियां सूचना सुरक्षा परिचालन समिति द्वारा अनुमोदित होंगी।

(ख) "संरक्षित प्रणाली" को प्रभावित करने वाले संजाल विन्यास में महत्वपूर्ण परिवर्तनों को सूचना सुरक्षा परिचालन समिति द्वारा अनुमोदित किया जाएगा।

(ग) "संरक्षित प्रणाली" के अनुप्रयोगों में प्रत्येक महत्वपूर्ण परिवर्तन को सूचना सुरक्षा परिचालन समिति द्वारा अनुमोदित किया जाएगा।

(घ) सूचना सुरक्षा परिचालन समिति के साथ "संरक्षित प्रणाली" से संबंधित साइबर घटना(घटनाएं) के समयबद्ध संचार के लिए एक तंत्र स्थापित किया जाएगा।

(ड़) "संरक्षित प्रणाली" के सभी सूचना सुरक्षा लेखापरीक्षाओं और अनुपालनों के परिणाम सूचना सुरक्षा परिचालन समिति के साथ साझा करने के लिए एक तंत्र स्थापित किया जाएगा।

(च) प्रत्येक दो वर्ष के पश्चात "संरक्षित प्रणाली" के सत्यापन के लिए विधिमान्यकरण ।

(3) "संरक्षित प्रणाली" रखने वाला संगठन अधोलिखित कार्य करेगा:

(क) एक अधिकारी को मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) के रूप में नामीनिर्दिष्ट करेगा जिसकी भूमिकाएं और उत्तरदायित्व एनसीआईआईपीसी द्वारा जारी नवीनतम "विवेचित सूचना अवसंरचना के संरक्षण के लिए दिशानिर्देश" और "भारत में महत्वपूर्ण क्षेत्रों के मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओस) की भूमिकाएं और उत्तरदायित्व " के अनुसार होंगी;

(ख) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र द्वारा जारी किए गए "विवेचित सूचना अवसंरचना के संरक्षण के लिए दिशानिर्देशों" या उद्योग द्वारा स्वीकृत मानकों जो कि उक्त राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र द्वारा विधिवत सम्यक रूप से किये गए हों, के अनुसार "संरक्षित प्रणाली" की सूचना सुरक्षा प्रबंधन प्रणाली (आईएसएमएस) की योजना बनायेगा, उसको स्थापित करेगा, कार्यान्वित करेगा, संचालित करेगा, उसकी निगरानी करेगा, समीक्षा करेगा, उसका रखरखाव करेगा और उसमे सतत सुधार करेगा;

(ग) सुनिश्चित करेगा कि "संरक्षित प्रणाली" की संजाल वास्तुकला प्रलेखित है । इसके अलावा, संगठन सुनिश्चित करेगा कि "संरक्षित प्रणाली" राष्ट्रीय विवेचित सूचना अवसंरचना संरक्षण केंद्र के नवीनतम "विवेचित सूचना अवसंरचना के संरक्षण के लिए दिशानिर्देशों" के अनुसार स्थिर, लचीला और मापनीय है। संजाल वास्तुकला में कोई भी परिवर्तन प्रलेखित किया जाना चाहिए;

(घ) "संरक्षित प्रणाली" तक पहुंच रखने वाले प्राधिकृत कर्मियों के प्रलेखन की योजना बनाएगा, उनको विकसित करेगा, उनका रखरखाव करेगा, और एक वर्ष में कम से कम एक बार या जब भी आवश्यक हो, या खंड (ख) में सुझाई गई सूचना सुरक्षा प्रबंधन प्रणाली के अनुसार उनकी समीक्षा करेगा;

(ड़) "संरक्षित प्रणाली" से संबंधित हार्डवेयर और सॉफ़्टवेयर की वस्तुसूची के दस्तावेजों की योजना बनाएगा, उनको विकसित करेगा, उनका रखरखाव करेगा और उनकी समीक्षा करेगा;

(च) सुनिश्चित करेगा कि "संरक्षित प्रणाली" की साइबर सुरक्षा वास्तुकला के लिए भेद्यता/ ख़तरा / जोखिम (वी / टी / आर) विश्लेषण वर्ष में कम से कम एक बार किया जायेगा। इसके अलावा, प्रणाली में महत्वपूर्ण परिवर्तन या उन्नयन होने पर भी सूचना सुरक्षा अभिचालन समिति को अवगत कराते हुए वी / टी / आर विश्लेषण शुरू किया जाएगा;

(छ) राष्ट्रीय विवेचित सूचना अवसंरचना संरक्षण केंद्र के साथ निकट समन्वय में साइबर आपात प्रबंधन योजना (सीसीएमपी) की योजना बनाएगा, उसको स्थापित करेगा, उसे कार्यान्वित करेगा, उसे संचालित करेगा, उसकी निगरानी करेगा, समीक्षा करेगा और उसमें लगातार सुधार करेगा;

(ज) खण्ड (ख) में सुझाई गई सूचना सुरक्षा प्रबंधन प्रणाली (आईएसएमएस) के अनुसार आवधिक आंतरिक और बाह्य सूचना सुरक्षा लेखा-परीक्षण का आचरण करेगा। राष्ट्रीय विवेचित सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) द्वारा "निजी / सरकारी संगठन द्वारा सीआईआई / संरक्षित प्रणालियों के लेखा-परीक्षण" के लिए जारी मानक संचालन प्रक्रिया (एसओपी) का दृढ़ता से पालन किया जाएगा;

(झ) सूचना प्रौद्योगिकी सुरक्षा सेवा स्तर करारों (एसएलएएस) के लिए प्रलेखित प्रक्रिया की योजना बनाएगा, उसको विकसित करेगा, उसका रखरखाव करेगा और उसकी समीक्षा करेगा। सेवा प्रदाताओं के साथ एसएलएएस को परिकल्पित करते समय इन प्रलेखित प्रक्रियायों का दृढ़ता से पालन किया जाएगा;

(ञ) उन्नत और उभरते हुए साइबर खतरों के विरुद्ध सुरक्षा के लिए निवारक, भेदिया और सुधारात्मक नियंत्रणों को लागू करने के लिए उपकरण और तकनीकों का उपयोग करके एक साइबर सुरक्षा संचालन केंद्र साइबर सुरक्षा संचालन स्थापित करेगा। इसके अतिरिक्त, साइबर सुरक्षा संचालन को नियमित आधार पर लॉग का विश्लेषण करके "संरक्षित प्रणाली" पर अनधिकृत पहुंच की पहचान करने और "संरक्षित प्रणाली" पर असामान्य और दुर्भावनापूर्ण क्रियाकलापों की पहचान करने के लिए उपयोग किया जाएगा। अनधिकृत पहुंच, असामान्य और दुर्भावनापूर्ण गतिविधि के अभिलेख, यदि कोई हो, तो उन्हें प्रलेखित किया जाएगा;

(ट) निरंतर संजाल उपलब्धता और प्रदर्शन सुनिश्चित करने के लिए "संरक्षित प्रणाली" के संजाल(लों) का नियंत्रण करने, प्रबंधन करने और निगरानी करने के लिए उपकरणों और तकनीकों का उपयोग करके एक संजाल संचालन केंद्र (एनओसी) की स्थापना करेगा;

(ठ) वह "संरक्षित प्रणाली" का समर्थन करने वाले संजाल उपकरणों, परिधि उपकरणों, संचार उपकरणों, सर्वर, प्रणालियों और सेवाओं के लॉग्स के नियमित बैकअप लेने की प्रक्रिया की योजना, विकास, रखरखाव और समीक्षा करेगा और खण्ड (ख) में सुझाई गई सूचना सुरक्षा प्रबंधन प्रणाली (आईएसएमएस) के अनुसार लॉग्स को संभाला जाएगा।

4. राष्ट्रीय विवोचित सूचना अवसंरचना संरक्षण केंद्र के प्रति "संरक्षित प्रणाली(यों)" की भूमिकाएं और उत्तरदायित्व:

(1) मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) राष्ट्रीय विवेचित सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) के साथ नियमित संपर्क बनाए रखेगा और संचार के सभी उपलब्ध या उचित तरीकों का उपयोग करते हुए उक्त राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र द्वारा सुझाए गए सुरक्षा के उपायों को कार्यान्वित करने के लिए ज़िम्मेदार होगा।

(2) मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) निम्नलिखित को साझा करेगा, जब भी इनमें कोई परिवर्तन होगा, या राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) द्वारा अपेक्षित होगा, और वह उक्त राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र द्वारा सुझाए गए आदानों/ प्रतिपुष्टियों को समाविष्ट करेगा:-

(क) विवेचित सूचना अवसंरचना (सीआईआई) का विवरण जिसे "संरक्षित प्रणाली" के रूप में घोषित किया गया है, जिसमें उक्त महत्वपूर्ण सूचना अवसंरचना पर और की निर्भरताएँ शामिल हैं।

(ख) "संरक्षित प्रणाली" की सूचना सुरक्षा संचालन समिति (आईएसएससी) के ब्यौरे।

(ग) "संरक्षित प्रणाली" की सूचना सुरक्षा प्रबंधन प्रणाली (आईएसएमएस)

(घ) "संरक्षित प्रणाली" की संजाल वास्तुकला।

(ड) "संरक्षित प्रणाली" तक पहुंच वाले प्राधिकृत कर्मी।

(च) "संरक्षित प्रणाली" से संबंधित हार्डवेयर और सॉफ्टवेयर की वस्तुसूची ।

(छ) "संरक्षित प्रणाली" की साइबर सुरक्षा वास्तुकला के लिए भेद्यता/ ख़तरा / जोखिम (वी / टी / आर) विश्लेषण के ब्यौरे।

(ज) "संरक्षित प्रणाली " के सूचना प्रौघोगिकी की सुरक्षा सेवा स्तर करार (एस एल एएस)

(3) (क) राष्ट्रीय विवेचित सूचना अवसंरचना संरक्षण केंद्र (एनआईसीआईपीसी) के साथ "संरक्षित प्रणाली" के लॉग्स को साझा करने के लिए मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ), एनसीआईआईपीसी के परामर्श से एक प्रक्रिया स्थापित करेगा ताकि विसंगतियों का पता लगाया जा सके और वास्तविक समय के आधार पर खतरे की खुफिया जानकारी उत्पन्न की जा सके।

(ख) मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) "संरक्षित प्रणाली" से संबंधित दिशा निर्देशों, सलाहों और भेद्यताओं, लेखा-परीक्षा टिप्पणियों आदि के मुद्दों को सुलझाने के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र के साथ "संरक्षित प्रणाली" की सी-एसओसी (अनधिकृत पहुंच, असामान्य और दुर्भावनापूर्ण क्रियाकलाप से संबंधित) के प्रलेखित अभिलेख साझा करने की एक प्रक्रिया को स्थापित करेगा।

(4) (क) मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) के परामर्श से "सुरक्षित प्रणाली" पर घटित साइबर घटना(ओं) के उक्त राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र को समय पर संचार के लिए एक प्रक्रिया स्थापित करेगा।

(ख) इसके अतिरिक्त, "संरक्षित प्रणाली" पर साइबर घटना(ओं) के मामले में घटना की प्रतिक्रिया पर राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र की नवीनतम मानक परिचालन प्रक्रिया (एसओपी) का दृढ़ता से पालन किया जाएगा।

[सं. 1(4)/2016-सीएलएफई]

एस. गोपालकृष्णन, संयुक्त सचिव

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

NOTIFICATION

New Delhi, the 22nd May, 2018

S. O. 2235(E).—In exercise of powers conferred by clause (zb) of sub-section (2) of section 87 read with section 70 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following Rules for the Information Security Practices and Procedures for Protected System, namely:-

1. Short Title and Commencement.

(1) These rules may be called the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

(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) "Chief Information Security Officer" means the designated employee of Senior management, directly reporting to Managing Director /Chief Executive Officer/Secretary of the organisation, having knowledge of information security and related issues, responsible for cyber security efforts and initiatives including planning, developing, maintaining, reviewing and implementation of Information Security Policies;

(c) "Critical Information Infrastructure" means Critical Information Infrastructure as referred to in explanation of sub-section (1) of section 70 of the Act;

(d) "Cyber Crisis Management Plan" outlines a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad-based approach for rapid identification,

information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical processes;

(e) "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 health or safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation;

(f) "Information Security Management System" means a set of policies, processes and procedures to establish, implement, operate, monitor, review, maintain and continually improve information security and minimize the risks by developing, maintaining, implementing and reviewing the adequate and appropriate security controls;

(g) "Information Security Steering Committee" means the committee comprising higher management officials of the organisation, responsible for continuously improving and strengthening the cyber security posture of the Protected System and also plan, develop, review remedial actions to mitigate and recover from malicious cyber incidents;

(h) "IT Security Service Level Agreements" means the legally recognised Service Level Agreements between the service providers and officials related to the "Protected System" for securing information related to "Protected System";

(i) "National Critical Information Infrastructure Protection Centre" means the agency established under sub-section (1) of section 70A of the Act;

(j) "Organisation" means-

(i) Ministries or Departments of the Government of India, State Governments and Union territories;

(ii) any agency of the Central Government, State Governments and Union territories;

(iii) any other entity having a 'Protected System'.

(k) "Protected System" means any computer, computer system or computer network of any organisationas notified under section 70 of the Act, in the official gazette by appropriate Government.

(l) "Service Provider" means any authorised individual(s), Government organisation, Public Sector Units(PSU), private agency, private company, partnership firm or any other body or agency providing services for the smooth and continuous functioning of the 'Protected System'.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Information Security Practices and Procedures for "Protected System".

(1) (a) The organisation having "Protected System" shall constitute an Information Security Steering Committee under the chairmanship of Chief Executive Officer/Managing Director/Secretary of the organisation.

(b) The composition of Information Security Steering Committee(ISSC) shall be as under:

(i) IT Head or equivalent;

(ii) Chief Information Security Officer (CISO);

(iii) Financial Advisor or equivalent;

(iv) Representative of National Critical Information Infrastructure Protection Centre (NCIIPC);

(v) Any other expert(s) to be nominated by the organisation.

(2) The Information Security Steering Committee (ISSC) shall be the apex body with roles and responsibilities as follows: -

(a) All the Information Security Policies of the "Protected System "shall be approved by Information Security Steering Committee.

(b) Significant changes in network configuration impacting "Protected System" shall be approved by the Information Security Steering Committee.

(c) Each significant change in application(s) of the "Protected System" shall be approved by Information Security Steering Committee.

(d) A mechanism shall be established for timely communication of cyber incident(s) related to "Protected System" to Information Security Steering Committee.

(e) A mechanism shall be established to share the results of all information security audits and compliance of "Protected System" to Information Security Steering Committee.

(f) Assessment for validation of "Protected System" after every two years.

(3) The organisation having "Protected System" shall

(a) nominate an officer as Chief Information Security Officer (CISO) with roles and responsibilities as per latest "Guidelines for Protection of Critical Information Infrastructure" and "Roles and Responsibilities of Chief Information Security Officers (CISOs) of Critical Sectors in India" released by NCIIPC;

(b) plan, establish, implement, operate, monitor, review, maintain and continually improve Information Security Management System (ISMS) of the "Protected System" as per latest "Guidelines for Protection of Critical Information Infrastructure" released by the National Critical Information Infrastructure Protection Centre or an industry accepted standard duly approved by the said National Critical Information Infrastructure Protection Centre;

(c) ensure that the network architecture of "Protected System" shall be documented. Further, the organisation shall ensure that the "Protected System" is stable, resilient and scalable as per latest National Critical Information Infrastructure Protection Centre "Guidelines for Protection of Critical Information Infrastructure". Any changes to network architecture shall be documented;

(d) plan, develop, maintain the documentation of authorised personnel having access to "Protected System" and the same shall be reviewed at least once a year, or whenever required, or according to the Information Security Management System(ISMS) as suggested in clause(b);

(e) plan, develop, maintain and review the documents of inventory of hardware and software related to "Protected System";

(f) ensure that Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of "Protected System" shall be carried out at least once a year. Further, Vulnerability/Threat/Risk (V/T/R) Analysis shall be initiated whenever there is significant change or upgrade in the system, under intimation to Information Security Steering Committee;

(g) plan, establish, implement, operate, monitor, review, and continually improve Cyber Crisis Management Plan (CCMP) in close coordination with National Critical Information Infrastructure Protection Centre;

(h) ensure conduct of internal and external Information Security audits periodically according to Information Security Management System(ISMS) as suggested in clause (b). The Standard

Operating Procedure (SOP) released by National Critical Information Infrastructure Protection Centre (NCIIPC) for "Auditing of CIIs/Protected Systems by Private/Government Organisation" shall be strictly followed;

(i) plan, develop, maintain and review documented process for IT Security Service Level Agreements (SLAs). The same shall be strictly followed while designing the Service Level Agreements with service providers;

(j) establish a Cyber Security Operation Center (C-SOC) using tools and technologies to implement preventive, detective and corrective controls to secure against advanced and emerging cyber threats. In addition, Cyber Security Operation Center is to be utilised for identifying unauthorized access to "Protected System", and unusual and malicious activities on the "Protected System", by analyzing the logs on regular basis. The records of unauthorised access, unusual and malicious activity, if any, shall be documented;

(k) establish a Network Operation Center (NOC) using tools and techniques to manage control and monitor the network(s) of "Protected System" for ensuring continuous network availability and performance;

(l) plan, develop, maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, communication devices, servers, systems and services supporting "Protected System" and the logs shall be handled as per the Information Security Management System(ISMS) as suggested in clause (b).

4. Roles and Responsibilities of "Protected System(s)" towards National Critical Information Infrastructure Protection Centre:-

(1) The Chief Information Security Officer (CISO) shall maintain regular contact with the National Critical Information Infrastructure Protection Centre(NCIIPC) and will be responsible for implementing the security measures suggested by the saidNational Critical Information Infrastructure Protection Centre(NCIIPC) using all available or appropriate ways of communication.

(2) The Chief Information Security Officer (CISO) shall share the following, whenever there is any change, or as required by the National Critical Information Infrastructure Protection Centre (NCIIPC), and incorporate the inputs/feedbacks suggested by the said National Critical Information Infrastructure Protection Centre (NCIIPC):-

(a) Details of Critical Information Infrastructure (CII)declared as "Protected System", including dependencies on and of the saidCritical Information Infrastructure.

(b) Details of Information Security Steering Committee (ISSC) of "Protected System".

(c) Information Security Management System (ISMS) of "Protected System".

(d) Network Architecture of "Protected System".

(e) Authorised personnel having access to "Protected System".

(f) Inventory of Hardware and Software related to "Protected System".

(g) Details of Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of "Protected System".

(h) Cyber Crisis Management Plan(CCMP).

(i) Information Security Audit Reports and post Audit Compliance Reports of "Protected System".

(j) IT Security Service Level Agreements (SLAs) of "Protected System".

(3) (a) The Chief Information Security Officer (CISO) shall establish a process, in consultation with the National Critical Information Infrastructure Protection Centre (NCIIPC), for sharing of logs of

"Protected System" with National Critical Information Infrastructure Protection Centre (NCIIPC) to help detect anomalies and generate threat intelligence on real time basis.

(b) The Chief Information Security Officer shall also establish a process of sharing documented records of Cyber Security Operation Center (related to unauthorised access, unusual and malicious activity) of "Protected System" with National Critical Information Infrastructure Protection Centre(NCIIPC) to facilitate issue of guidelines, advisories and vulnerability, audit notes etc. relating to "Protected System".

(4) (a) The Chief Information Security Officer (CISO) shall establish a process in consultation with National Critical Information Infrastructure Protection Centre (NCIIPC), for timely communication of cyber incident(s) on "Protected System" to the said National Critical Information Infrastructure Protection Centre (NCIIPC).

(b) In addition, National Critical Information Infrastructure Protection Centre's latest Standard Operating Procedure (SOP) on Incident Response shall be strictly followed in case of cyber incident(s) on "Protected System".

[No. 1(4)/2016-CLFE]

S. GOPALAKRISHNAN, Jy. Secy.

RAKESH SUKUL Digitally signed by RAKESH SUKUL Date: 2018.06.05 20:05:11 +05'30'

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-27072023-247654
CG-DL-E-27072023-247654

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 3230] नई दिल्ली, बृहस्पतिवार, जुलाई 27, 2023/श्रावण 5, 1945
No. 3230] NEW DELHI, THURSDAY, JULY 27, 2023/SHRAVANA 5, 1945

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

अधिसूचना

नई दिल्ली, 27 जुलाई, 2023

का.आ. 3376(अ).—केंद्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 70 की उप-धारा (1) और उप-धारा (2) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, अखिल भारतीय आयुर्विज्ञान संस्थान, नई दिल्ली की नाजुक सूचना अवसंरचना होने के कारण अस्पताल प्रबंधन सूचना प्रणाली, प्रयोगशाला प्रबंधन सूचना प्रणाली, पिक्चर आर्काइविंग एंड कम्युनिकेशन सिस्टम और ब्लड बैंक प्रबंधन प्रणाली से संबंधित कंप्यूटर संसाधनों एवं इसके सहयुक्त आश्रितताओं के कंप्यूटर संसाधनों को उक्त अधिनियम के प्रयोजनों के लिए एतद्वारा संरक्षित प्रणाली घोषित करती है और निम्नलिखित व्यक्तियों को संरक्षित प्रणालियों तक पहुंच बनाने के लिए प्राधिकृत करती है, अर्थात् :-

(क) संरक्षित प्रणाली तक पहुंच बनाने के लिए, अखिल भारतीय आयुर्विज्ञान संस्थान नई दिल्ली द्वारा लिखित रूप में प्राधिकृत अखिल भारतीय आयुर्विज्ञान संस्थान, नई दिल्ली का कोई अभिहित कर्मचारी;

(ख) संविदात्मक प्रबंधित सेवा-प्रदाता या तृतीय पक्षकार विक्रेता के दल का कोई सदस्य जिसे आवश्यकता के आधार पर पहुंच बनाने के लिए अखिल भारतीय आयुर्विज्ञान संस्थान, नई दिल्ली द्वारा लिखित रूप में प्राधिकृत किया गया है;और

(ग) मामला दर मामला के आधार पर, अखिल भारतीय आयुर्विज्ञान संस्थान, नई दिल्ली द्वारा लिखित रूप में प्राधिकृत कोई परामर्शी, विनियामक, सरकारी पदाधिकारी, संपरीक्षक और पणधारी।

2. यह अधिसूचना राजपत्र में इसके प्रकाशन की तिथि से प्रभावी होगी।

[फा. सं. 2(5)/2022-सीएल-भाग(1)]

संदीप चटर्जी, वैज्ञानिक 'जी'

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

NOTIFICATION

New Delhi, the 27th July, 2023

S.O. 3376(E).—In exercise of the powers conferred by sub-sections (1) and (2) of section 70 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby declares the computer resources relating to the Hospital Management Information System, Laboratory Management Information System, Picture Archiving and Communication System and Blood Bank Management System, being Critical Information Infrastructure of the All India Institute of Medical Sciences, New Delhi, and the computer resources of its associated dependencies, to be protected systems for the purposes of the said Act and authorises the following persons to access the protected systems, namely:—

(a) any designated employee of the All India Institute of Medical Sciences, New Delhi authorised in writing by the All India Institute of Medical Sciences, New Delhi to access the protected system;

(b) any team member of contractual managed service provider or third-party vendor who have been authorised in writing by the All India Institute of Medical Sciences, New Delhi for need-based access; and

(c) any consultant, regulator, Government official, auditor and stakeholder authorised in writing by the All India Institute of Medical Sciences, New Delhi on case to case basis.

2. This notification shall come into force on the date of its publication in the Official Gazette.

[F. No. 2(5)/2022-CL-Part(1)]

SANDIP CHATTERJEE, SCIENTIST 'G'

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054. MANOJ KUMAR VERMA