(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.

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.