

संख्या:-841/78-1-2024-1099/89/2024

प्रेषक,

नेह्रू जैन,

विशेष सचिव,

उ०प्र० शासन।

सेवा में,

अपर मुख्य सचिव/प्रमुख सचिव/सचिव,

नगर विकास, खाद्य एवं रसद, समाज कल्याण, नियोजन, आवास एवं शहरी नियोजन, चीनी उद्योग एवं गन्ना विकास, स्टाम्प एवं रजिस्ट्रेशन, राज्य कर, विज्ञान एवं प्रौद्योगिकी, सूचना एवं जनसम्पर्क, पंचायतीराज, पर्यटन, सिंचाई एवं जल संसाधन, चिकित्सा शिक्षा एवं प्रशिक्षण, राजस्व, कृषि, अतिरिक्त ऊर्जा स्रोत, नियुक्ति, नागरिक उड्डयन, सहकारिता, दुग्धशाला विकास तथा ग्रामीण अभियन्त्रण विभाग, उ०प्र० शासन।

आई.टी. एवं इलेक्ट्रॉनिक्स अनुभाग-1

लखनऊ: दिनांक: 29 मई, 2024

विषय:- विभागीय स्तर पर चीफ इन्फॉर्मेशन सिस्टीम ऑफिसर (CISOs) नामित किये जाने के सम्बन्ध में।

महोदय

उपर्युक्त विषय के संबंध में अवगत कराना है कि प्रदेश सरकार के विभिन्न विभागों द्वारा विगत वर्षों में कोर आई०टी० एवं ई-गवर्नेन्स इन्फ्रास्ट्रक्चर को विकसित किया गया है, जिसका उपयोग कर आम जनमानस द्वारा सरकारी सेवाओं का लाभ इन्टरनेट के माध्यम से लिया जा रहा है, जिसके परिणामस्वरूप साइबर स्पेस में साइबर अटैक्स की सम्भावनाएँ भी प्रबल हो गयी हैं। इस संवेदनशील डाटा की वृद्धि निरन्तर हो रही है तथा इसके उपयोग एवं आदान-प्रदान में भी वृद्धि हो रही है, जिस हेतु इस संवेदनशील डाटा एवं एप्लीकेशन की सुरक्षा करना अत्यन्त आवश्यक हो गया है।

2- साइबर अपराधों व साइबर सुरक्षा विषयक स्टैक होल्डर्स डायलॉग की पुनर्समीक्षा तथा भविष्य पर विचार किये जाने हेतु मुख्य सचिव, उ०प्र० शासन की अध्यक्षता में दिनांक 04 अप्रैल, 2024 को समीक्षा बैठक (कार्यवृत्त संलग्नक-1) आयोजित की गयी। उक्त कार्यवृत्त के बिन्दु सं०-6 के अनुपालन में यह अपेक्षा की गयी है कि विभाग अपने स्तर से चीफ इन्फॉर्मेशन सिस्टीम ऑफिसर (डी०सी०आई०एस०ओ०) नामित कर उसकी सूचना आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र० शासन को उपलब्ध करायें।

3- इस संबंध में पूर्व में भी प्रबन्ध निदेशक, यू०पी० डेस्क के पत्र सं०-डी/23-24/3788 दिनांक 12 दिसम्बर, 2023 के साथ संलग्न आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र० शासन द्वारा विभागों को प्रेषित पत्र सं०-1461/78-01-2023-70आईटी/2017टीसी-1 दिनांक 29 सितम्बर, 2023 (संलग्नक-2) के माध्यम से विभागों में साइबर सुरक्षा की दृष्टि से शासकीय विभागों द्वारा CISO नामित करने का अनुरोध किया गया था, ताकि NCIIPC, भारत सरकार से ई-मेल के माध्यम से समय-समय पर प्राप्त होने वाली Advisory एवं Security Threads से सम्बन्धित सूचना सभी

को प्रेषित की जा सके। साथ ही भारत सरकार के पत्र सं०-20(3)/2022-CERT-In दिनांक 28 अप्रैल, 2022 (संलग्नक-3) को समस्त विभागों में सी०आई०एस०ओ० नामित किये जाने के दिशा-निर्देश जारी किये गये हैं।

4- भारत सरकार द्वारा महत्वपूर्ण / संवेदनशील डाटा तथा एप्लीकेशनन्स की सुरक्षा के दृष्टिगत इन्फॉर्मेशन सिक्योरिटी एक्ट 2000 की धारा 70ए के अन्तर्गत नेशनल क्रिटिकल इन्फॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेन्टर (एन०सी०आई०आई०पी०सी०) संस्था का गठन किया गया है, जिसे क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर के संरक्षण के संबंध में राष्ट्रीय नोडल एजेंसी के रूप में नामित किया गया है। यह संस्था क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर को सुरक्षा प्रदान करने की दिशा में कार्य करता है। एन०सी०आई०आई०पी०सी० के प्राथमिक कार्य जैसे-साइबर हमलों के विरुद्ध महत्वपूर्ण बुनियादी ढांचों को सुदृढ़ करना, वेनराबिलिटी एनॉलिसिस, इन्सीडेन्ट रिस्पॉन्स और कैपेसिटी बिल्डिंग सम्मिलित है। एन०सी०आई०आई०पी०सी० समय-समय पर राज्य के विभागीय पोर्टल के वेनराबिलिटी रिपोर्ट्स, थर्ड पार्टी साफ्टवेयर सिस्टम में प्राप्त वेनराबिलिटी रिपोर्ट तथा इंडीकेटर्स ऑफ काम्प्रोमाईज एडवाइजरी राज्य सी०आई०एस०ओ० के साथ ई-मेल पर साझा करता है।

5- इस सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि उपरोक्त तथ्यों की महत्ता को ध्यान में रखते हुए अपने विभाग में सी०आई०एस०ओ० निम्नलिखित प्रारूप पर नामित करते हुए, नामित अधिकारी की सूचना उपलब्ध कराते हुए उसकी एक प्रति सेण्टर फॉर ई-गवर्नेन्स, उत्तर प्रदेश, (उ०प्र० सरकार की समिति) प्रथम तल, अपट्रॉन विल्डिंग, निकट गोमती बैराज, गोमती नगर लखनऊ-226010 को भी तत्काल उपलब्ध कराना सुनिश्चित करें:-

नाम	पदनाम	गवर्नमेन्ट ई-मेल आई०डी० (gov/nic)	दूरभाष नं०
1	2	3	4

कृपया उपरोक्त निर्देशों का अनुपालन सुनिश्चित कराने का कष्ट करें।

संलग्नक: यथोक्त।

Digitally Signed by नेहा
जैन

Date: 27-05-2024 20:24:32

Reason: Approved

भवदीया,

(नेहा जैन)

विशेष सचिव।

पृ०संख्या-841(1)/78-1-2024, तददिनांक

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित:-

1-निजी सचिव, मुख्य सचिव, उ०प्र० शासन।

2-निजी सचिव, अपर मुख्य सचिव, मा० मुख्य मंत्री जी, उ०प्र०।

3- निजी सचिव, कृषि उत्पादन, उ०प्र०।

4-निजी सचिव, अवस्थापना विकास आयुक्त, उ०प्र०।

5-पुलिस महानिदेशक, उ०प्र०।

6-राज्य सूचना विज्ञान अधिकारी, (एस०आई०ओ०), एन०आई०सी०, योजना भवन, लखनऊ।

7-प्रबन्ध निदेशक, यूपीडेस्को, उ०प्र०।

8-राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स, उ०प्र०, अपट्टान बिल्डिंग, गोमती नगर, लखनऊ।

9-गार्ड फाइल।

भवदीया,
(नेहा जैन)
विशेष सचिव।

प्रेषक,

नेहा जैन,
विशेष सचिव,
उ0प्र0 शासन।

सेवा में,

समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव,
उत्तर प्रदेश शासन।

आई0टी0 एवं इलेक्ट्रॉनिक्स अनु0-1

लखनऊ: दिनांक: 29 सितम्बर, 2023

विषय:- विभागीय Chief Information Security Officer (CISO) की गवर्नमेन्ट ई-मेल आईडी प्रेषित कराये जाने के सम्बन्ध में।

महोदय/महोदया,

उपर्युक्त विषयक प्रबन्ध निदेशक, यूपीडेस्को के पत्र संख्या-D/23-24/2356, दिनांक 29-08-2023 के साथ संलग्न पूर्व में प्रेषित शासन के पत्र संख्या:-1143/78-01-2023 दिनांक 07.07.2023 (छायाप्रति संलग्न) का सन्दर्भ ग्रहण करने का कष्ट करें, जिसके माध्यम से विभागों में साइबर सुरक्षा की दृष्टि से शासकीय विभागों द्वारा CISO नामित करते हुए Chief Information Security Officer (CISO) की गवर्नमेन्ट ई-मेल आईडी उपलब्ध कराये जाने का अनुरोध किया गया था, ताकि NCIIPC से ई-मेल के माध्यम से समय-समय पर प्राप्त होने वाली Advisory एवं Security Threads (छायाप्रति संलग्न) से सम्बन्धित सूचना प्रेषित की जा सके।

2- अवगत कराना है कि उक्त पत्र के क्रम में अभी तक मात्र 18 विभागों के CISO का नामांकन प्राप्त हुआ है, जिसमें से मात्र 07 विभागों की गवर्नमेन्ट ई-मेल आईडी प्राप्त हुई है तथा 08 विभागों ने गवर्नमेन्ट ई-मेल आईडी के स्थान पर Gmail ID उपलब्ध करायी है, जबकि शेष विभागों द्वारा अभी तक नामित CISO व उनकी गवर्नमेन्ट ई-मेल आईडी उपलब्ध नहीं करायी गयी है।

3- इस संबंध में पुनः मुझे यह कहने का निदेश हुआ है कि कृपया अपने विभाग से नामित Chief Information Security Officer (CISO) तथा उनकी गवर्नमेन्ट ई-मेल आईडी सहित सूचना (यदि नामित नहीं है, तो नामित करते हुए) निम्नवत् प्रारूप पर उपलब्ध कराने का कष्ट करें।

नाम	पदनाम	गवर्नमेन्ट ई-मेल आईडी0	दूरभाष नं0
1	2	3	4

संलग्नक-यथोक्त।

भवदीया,

29.09.23
(नेहा जैन)
विशेष सचिव

संख्या एवं दिनांक तदैव

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ प्रेषित:-

- 1- प्रमुख सचिव, आई0टी0 एवं इले0 विभाग, उ0प्र0 शासन।
- 2- प्रबन्ध निदेशक, यूपीडेस्को, लखनऊ।

आज्ञा से,

(नेहा जैन)
विशेष सचिव

सन्दर्भ सं० : D/23-24/ 2356
दिनांक : 29.08.2023

सेवा में,
विशेष सचिव,
आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-2,
उत्तर प्रदेश शासन।

विषय- विभागीय Chief Information Security Officer (CISO) की गवर्नमेंट ई-मेल आईडी प्रेषित कराये जाने के सम्बन्ध में।

महोदय,

कृपया यूपीडेस्को के पत्रांक-D/23-24/0772 दिनांक 20.05.2023 एवं पत्रांक-D/23-24/1399 दिनांक 01.07.2023, जिसके द्वारा National Critical Information Infrastructure Protection Centre (NCIIPC) के विभिन्न तिथियों में विभागों से सम्बन्धित प्राप्त ई-मेल पत्र जो कि विभागीय Chief Information Security Officer (CISO) की गवर्नमेंट ई-मेल आईडी प्रेषित किये जाने से सम्बन्धित है, का सन्दर्भ ग्रहण करने का कष्ट करें। विभागों में साइबर सुरक्षा की दृष्टि से शासकीय विभागों द्वारा CISO नामित करते हुए Chief Information Security Officer (CISO) की गवर्नमेंट ई-मेल आईडी उपलब्ध कराये जाने हेतु अनुरोध किया गया था।

उक्त के क्रम में विशेष सचिव, आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-1, उत्तर प्रदेश शासन के पत्रांक-872/78-01-2023 दिनांक 22.05.2023 एवं पत्रांक-1143/78-1-2023 दिनांक 07.07.2023 के माध्यम से समस्त शासकीय विभागों को पत्र प्रेषित किया गया था, जिसके क्रम में कुल 18 CISO का नामांकन प्राप्त हुआ है जिसमें से मात्र 07 विभागों की गवर्नमेंट Mail ID, 08 विभागों की Gmail ID का उल्लेख है एवं 03 विभागों की Mail ID का उल्लेख नहीं है (संलग्नक)।

अनुरोध है कि शासन स्तर से उक्त 07 विभागों को छोड़कर शेष विभागों के CISO की गवर्नमेंट ई-मेल आईडी उपलब्ध कराये जाने हेतु पुनः पत्र प्रेषित करने का कष्ट करें।

संलग्नक : यथोक्त।

भवदीय,

(कुमार विनीत)
प्रबन्ध निदेशक

SO-1
20/08/2023
28/08/23
30.8.23

पत्रांक...../प्र.स.ग्रा.वि एवं प्रा.अभि.वि./2023

अनुस्मारक

संख्या:-1143/78-1-2023

प्रेषक,

कुमार विनीत,
विशेष सचिव/स्टेट CISO,
उ०प्र० शासन।

सेवा में,

समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव,
उत्तर प्रदेश शासन।

आईटी० एवं इलेक्ट्रॉनिक्स अनु०-1

लखनऊ, दिनांक: ०७ जुलाई, 2023

विषय:- विभागीय Chief Information Security Officer (CISO) की गवर्नमेंट ई-मेल आईडी प्रेषित कराये जाने के सम्बन्ध में।

महोदय/महोदया,

कृपया पूर्व में प्रेषित पत्र संख्या:-872/78-01-2023 दिनांक 22.05.2023 (छायाप्रति संलग्न) का सन्दर्भ ग्रहण करने का कष्ट करें, जिसके माध्यम से विभागों में साइबर सुरक्षा की दृष्टि से शासकीय विभागों द्वारा CISO नामित करते हुए Chief Information Security Officer (CISO) की गवर्नमेंट ई-मेल आईडी उपलब्ध कराये जाने का अनुरोध किया गया है, ताकि NCIIPC से ई-मेल के माध्यम से समय-समय पर प्राप्त होने वाली Advisory एवं Security Threads (छायाप्रति संलग्न) से सम्बन्धित सूचना प्रेषित की जा सके।

2. इस संबंध में मुझे यह कहने का निदेश हुआ है कि कृपया अपने विभाग से Chief Information Security Officer (CISO) नामित किये जाने की सूचना (यदि नामित नहीं है, तो नामित करते हुए) निम्नवत् प्रारूप पर उपलब्ध कराने का कष्ट करें।

नाम	पदनाम	ई-मेल आईडी०	दूरभाष नं०
1	2	3	4

संलग्नक-यथोक्त।

भवदीय,

(कुमार विनीत)

विशेष सचिव/स्टेट CISO

VS(SPO) संख्या एवं दिनांक तदैव

809

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ प्रेषित:-

1- प्रमुख सचिव, आईटी० एवं इले० विभाग, उ०प्र० शासन।

2- प्रबन्ध निदेशक, यूपीडेस्को, लखनऊ।

आज्ञा से,

(कुमार विनीत)

विशेष सचिव/स्टेट CISO

(हिमांशु कुमार)

अपर मुख्य सचिव

ग्राम्य विकास एवं ग्रामीण अभियंत्रण विभाग
उत्तर प्रदेश शासन

अनुसन्धित (अ.सि.वि.)
18.7.2023
18.7.2023
ग्राम्य विकास-2
18/7/23
RO-18/7/23

क्र.सं.	नाम	पदनाम	विभाग का नाम	ई-मेल आई.डी.	दूरभाष संख्या
1	श्री गुलाब सिंह	संयुक्त सचिव	अल्पसंख्यक कल्याण एवं वक्फ बोर्ड	singhgulab1963@gmail.com	9454411693
2	श्री मोहम्मद आसिम रिजवी,	अनु सचिव	भाषा विभाग	mohammad.13162@gov.in	9454413162
3	श्री अन्नावि दिनेशकुमार	विशेष सचिव	प्राविधिक, शिक्षा विभाग	splsectecedul@gov.in	8787085157
4	श्री सुमित मौर्य	सहायक उप नियंत्रक (व0वे0)	नागरिक सुरक्षा विभाग लखनऊ	suitmaurya2110@gmail.com	9919191296
5	श्री रघुनाथ प्रसाद वर्मा	अनु सचिव	संस्कृति विभाग, उ.प्र. शासन	culture.section523@gmail.com	9454412291
6	श्री पूणदिव उपाध्याय	विशेष सचिव	वित्त (व्यय-नियंत्रण) विभाग	pdupadhyay15964@gmail.com	9412581273
7	श्री आलोक कुशवाहा	सहायक निदेशक	ग्राम्य विकास विभाग	alok.43609@gov.in	8765957412
8	श्री प्रतीश प्रांजल	अधिसासी अभियंता (आई.टी.)	उ.प्र. पावर कारपोरेशन लिमिटेड	cisouppcl@gmail.com	9651554444
9	श्री श्याम मोहन तिवारी	संयुक्त सचिव	राष्ट्रीय एकीकरण विभाग	shyammohan082410@gmail.com	9454411673
10	श्री राजेन्द्र राम	उप सचिव	ग्राम्य विकास विभाग	rjendra.12938@gov.in	9454412938
11	श्री उमेश कुमार तिवारी	संयुक्त सचिव	आबकारी विभाग	umesh.13881@gov.in	9454413881
12	श्री सुनील कुमार पाण्डेय	विशेष सचिव	खादी एवं ग्रामोद्योग विभाग	sunil.13449@gov.in	
13	डा० सरोज कुमार	विशेष सचिव	सचिवालय प्रशासन विभाग	saroj.kumar@nic.in	
14	श्री अजातशत्रु शाही	उपनिदेशक	युवा कल्याण एवं प्रान्तीय रक्षक दल/विकास दल महानिदेशालय, उत्तर प्रदेश लखनऊ		
15	श्री सत्येन्द्र कुमार तिवारी	सिस्टम एनालिस्ट	राज्य कृषि उत्पादन मण्डी परिषद लखनऊ		765956961
16	श्री आशुतोष द्विवेदी	विशेष सचिव	लोक निर्माण विभाग	vsadpwd22@gmail.com	9415531989
17	श्री राकेश कुमार	संयुक्त सचिव	न्याय विभाग		
18	श्री प्रकाश चन्द्र अग्रवाल	अनु सचिव	राजनैतिक पेंशन विभाग, उ.प्र. शासन	politicalpensionupgov@gmail.com	9454412851

No. 20(3)/2022-CERT-In
Government of India
Ministry of Electronics and Information Technology (MeitY)
Indian Computer Emergency Response Team (CERT-In)

Electronics Niketan,
6 CGO Complex,
New Delhi-110003

Dated: 28 April, 2022

Subject: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

Whereas, the Central Government in terms of the provisions of sub-section (1) of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000) has appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette and as per provisions of sub-section (4) of section 70B of IT Act, 2000 The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:-

- a) collection, analysis and dissemination of information on cyber incidents;
- b) forecast and alerts of cyber security incidents;
- c) emergency measures for handling cyber security incidents;
- d) coordination of cyber incidents response activities;
- e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- f) such other functions relating to cyber security as may be prescribed.

And whereas, "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" were notified and published vide notification dated 16.01.2014 by the Central Government 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 IT Act, 2000.

And whereas, as per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000.

And whereas, various instances of cyber incidents and cyber security incidents have been and continue to be reported from time to time and in order to coordinate response activities as well as emergency measures with respect to cyber security incidents, the requisite information is either sometime not found available or readily not available with service providers/data centres/body corporate and the said primary information is essential to carry out the analysis, investigation and coordination as per the process of law.

And whereas, it is considered expedient in the interest of the 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 any cognizable offence using computer resource or for handling of any cyber incident, that following directions are issued to augment and strengthen the cyber security in the country:

- (i) All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC.
- (ii) Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.

- (iii) When required by order/direction of CERT-In, for the purposes of cyber incident response, protective and preventive actions related to cyber incidents, the service provider/intermediary/data centre/body corporate is mandated to take action or provide information or any such assistance to CERT-In, which may contribute towards cyber security mitigation actions and enhanced cyber security situational awareness. The order / direction may include the format of the information that is required (up to and including near real-time), and a specified timeframe in which it is required, which should be adhered to and compliance provided to CERT-In, else it would be treated as non-compliance of this direction. The service providers, intermediaries, data centres, body corporate and Government organisations 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 at Annexure II 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.
- (iv) All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.
- (v) Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:
- a. Validated names of subscribers/customers hiring the services
 - b. Period of hire including dates
 - c. IPs allotted to / being used by the members
 - d. Email address and IP address and time stamp used at the time of registration / on-boarding
 - e. Purpose for hiring services
 - f. Validated address and contact numbers
 - g. Ownership pattern of the subscribers / customers hiring services

- (vi) The virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years so as to ensure cyber security in the area of payments and financial markets for citizens while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets.

For the purpose of KYC, the Reserve Bank of India (RBI) Directions 2016 / Securities and Exchange Board of India (SEBI) circular dated April 24, 2020 / Department of Telecom (DoT) notice September 21, 2021 mandated procedures as amended from time to time may be referred to as per Annexure III.

With respect to transaction records, accurate information shall be maintained in such a way that individual transaction can be reconstructed along with the relevant elements comprising of, but not limited to, information relating to the identification of the relevant parties including IP addresses along with timestamps and time zones, transaction ID, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred.

And whereas, the meaning to the terms 'cyber incident' or 'cyber security incident' or 'computer resource' or other terms may be ascribed as defined in the IT Act, 2000 or "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" as the case may be.

And whereas, in case of any incident, the above-referred entities must furnish the details as called for by CERT-In. The failure to furnish the information or non-compliance with the ibid. directions, may invite punitive action under sub-section (7) of the section 70B of the IT Act, 2000 and other laws as applicable.

This direction will become effective after 60 days from the date on which it is issued.

Annexure I

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:

[Refer Rule 12(1)(a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013]

- i. Targeted scanning/probing of critical networks/systems
- ii. Compromise of critical systems/information
- iii. Unauthorised access of IT systems/data
- iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- v. Malicious code attacks such as spreading of virus/worm/Trojan/Bots/Spyware/Ransomware/Cryptominers
- vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers
- vii. Identity Theft, spoofing and phishing attacks
- viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- ix. Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
- x. Attacks on Application such as E-Governance, E-Commerce etc.
- xi. Data Breach
- xii. Data Leak
- xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
- xiv. Attacks or incident affecting Digital Payment systems
- xv. Attacks through Malicious mobile Apps
- xvi. Fake mobile Apps
- xvii. Unauthorised access to social media accounts
- xviii. Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications
- xix. Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones

xx. Attacks or malicious/ suspicious activities affecting systems/
servers/software/ applications related to Artificial Intelligence and Machine
Learning

The incidents can be reported to CERT-In via email (incident@cert-in.org.in),
Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and
formats of reporting cyber security incidents is also published on the website of
CERT-In www.cert-in.org.in and will be updated from time to time.

Annexure II

Format for providing Point of Contact (PoC) information by Service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In

The Information relating to the Point of Contact shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified below and shall be updated from time to time:

Name	
Designation	
Organisation Name	
Office Address	
Email ID	
Mobile No.	
Office Phone	
Office Fax	

Annexure III

KYC Requirements

For the purpose of KYC, any of following Officially Valid Document (OVD) as a measure of identification procedure prescribed by the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016 / Securities and Exchange Board of India Clarification on Know Your Client (KYC) Process and Use of Technology for KYC vide Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020 / The Department of Telecom File No: 800-12/2021- AS.II dated September 21, 2021 on Self-KYC (S-KYC) as an alternate process for issuing of new mobile connections to Local and Outstation category customers, shall be used and maintained:

- a. The passport,
- b. The driving license,
- c. Proof of possession of Aadhaar number,
- d. The Voter's Identity Card issued by the Election Commission of India,
- e. Job card issued by NREGA duly signed by an officer of the State Government and
- f. Letter issued by the National Population Register containing details of name and address.
- g. Validated phone number
- h. Trading account number and details, Bank account number and bank details

For the purpose of KYC for business entities (B2B), documents mentioned in the Customer Due Diligence (CDD) process prescribed in Reserve Bank of India Master Direction - Know Your Customer (KYC) Direction, 2016 as updated from time to time shall be used and maintained.

1/541141/2024

साइबर अपराधों व साइबर सुरक्षा विषयक स्टेकहोल्डर्स डायलॉग की पुनर्समीक्षा तथा भविष्य की रणनीति पर विचार करने हेतु मुख्य सचिव, उ०प्र० शासन की अध्यक्षता में दिनांक 04.04.2024 को अपराह्न 6.30 बजे, आहूत प्रस्तुतीकरण बैठक के सम्बन्ध में।

उक्त आहूत प्रस्तुतीकरण बैठक में निम्नलिखित अधिकारियों द्वारा प्रतिभाग किया गया:

1. श्री दीपक कुमार, अपर मुख्य सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
2. श्री प्रशान्त कुमार, पुलिस महानिदेशक, उ०प्र०।
3. श्री नवीन अरोड़ा, अपर पुलिस महानिदेशक, तकनीकी सेवार्य, उ०प्र०।
4. श्री संजीव गुप्ता, सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
5. श्री अनुराग यादव, सचिव, नियोजन विभाग, उ०प्र० शासन।
6. श्री ए.वी. राजामौलि, सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
7. श्रीमती रूपा एम० निदेशक, I4C, गृह मंत्रालय, भारत सरकार, नयी दिल्ली.
8. श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ०प्र०।
9. श्री योगेश कुमार, विशेष सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
10. श्रीमती नेहा जैन, विशेष सचिव, आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र० शासन।
11. श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ०प्र०।

प्रश्नगत प्रकरण में अमर शहीद चन्द्रशेखर आजाद, प्रेक्षागृह, भू-तल, सिग्नेचर बिल्डिंग (PHQ), लखनऊ में आहूत विस्तृत प्रस्तुतीकरण निम्नलिखित विशेषज्ञों द्वारा किया गया:

क्र०सं०	वक्ता का नाम/ पदनाम	विषय
01	श्री अभिषेक सिंह, अपर सचिव, एम०ई०आई०टी०, भारत सरकार।	Cyber Crime & Cyber Security Emerging Challenges & Strategy For Future.
02	श्री जी. के. गोस्वामी, अपर पुलिस महानिदेशक, फॉरेंसिक, उ०प्र०।	Cyber Crime & Cyber Security Role of Forensic Science
03	श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ०प्र०	Cyber Crime in Uttar Pradesh.
04	श्री सुबोध कुमार, CEO, CERT-IN, GOI	Role of CERT-IN- Incident Response
05	श्रीमती रूपा एम० निदेशक, I4C	Presentation of Cyber Crimes by I4C MHA
06	श्रीमती नेहा जैन, विशेष सचिव, आई०टी० एवं	Proposed UP Cyber Security Policy, C SIRT-UP, Role of CISOs

I/541141/2024

	इलेक्ट्रॉनिक्स विभाग, उ०प्र० शासन।	
07	श्री बालू केन्चप्पा, R.D., R.B.I., KANPUR	Cyber Security, Customer Education & Protection- Role of RBI

उक्त प्रस्तुतीकरण/व्याख्यान के समापन के बाद मुख्य सचिव महोदय द्वारा प्रकरण से भिन्न वरिष्ठ अधिकारियों के साथ की गयी बैठक में गहन विचार विमर्शपरान्त अधोलिखित बिन्दुओं पर कार्यवाही किये जाने का निर्णय लिया गया:-

(1) प्रकरण में भारत सरकार के सूचना एवं प्रौद्योगिकी मंत्रालय के अधीन स्थापित CERT-IN की भाँति उ०प्र० में STATE CERT (S-CERT) स्थापित किया जाये एवं जिसे National Cyber Coordination Centre (NCCC) तथा साइबर स्वच्छता केन्द्र (CSK) के साथ समन्वय का कार्य सौंपा जाए।

(कार्यवाही- आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र०)

(2) प्रदेश में साइबर सुरक्षा को दृष्टिगत रखते हुए एस-सर्ट (S-CERT) की सुचारु रूप से स्थापना किये जाने तथा बेहतर क्रियाशीलता हेतु 02-02 सदस्यों की टीम (उप पुलिस महानिरीक्षक, साइबर क्राइम, व एक अन्य तथा CISO आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र० व एक अन्य) संरचना व प्रणाली में उत्कृष्ट कार्य कर रहे राज्य का भ्रमण कर उन राज्यों में स्थापित एस-सर्ट (S-CERT) की संरचना एवं उपयोग में लाये जा रहे सर्वोत्तम संव्यवहारों की सूचना/जानकारी प्राप्त की जाए। इस सम्बन्ध में CERT-IN संस्था का भी भ्रमण किया जाए एवं महानिदेशक, CERT-IN से अपेक्षित सहयोग प्राप्त किया जाए।

(कार्यवाही- आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र० पुलिस महानिदेशक, साइबर क्राइम, उ०प्र०)

(3) उ०प्र० के साथ ही राष्ट्रीय परिदृश्य पर डिजिटल क्रांति के प्रसार को देखते हुए प्रदेश में SOC (Security Operations Center) एवं NOC (Network Operations Center) की स्थापना की जाए, जिससे साइबर सुरक्षा को भविष्य की आवश्यकताओं के दृष्टिगत मजबूत बनाया जा सके।

(कार्यवाही- आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र०)

(4) बैठक में साइबर सुरक्षा के दृष्टिगत उ०प्र० राज्य में CII (Critical Information Infrastructure) का पूर्ण चिन्हांकन कर लिया जाए एवं CII की सुरक्षा किस प्रकार से सुनिश्चित की जायेगी, के सम्बन्ध में विभागों हेतु SOP (Standard Operating Procedure) बनायी जाए।

(कार्यवाही- आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र०)

(5) साइबर अपराधों से सम्बन्धित अन्वेषण की कार्यवाही गुणात्मक आधार पर सम्पन्न की जा सके, इस हेतु State Forensic Lab U/S 79 A of IT Act को अधिसूचित किया जाए।

(कार्यवाही- अपर पुलिस महानिदेशक, तकनीकी सेवाएँ, उ०प्र० तथा गृह (पुलिस) अनुभाग-9)

(6) साइबर सुरक्षा को मजबूत करने एवं साइबर अपराधों पर प्रभावी अंकुश लगाये जाने के दृष्टिगत प्रदेश के समस्त विभागों में सी०आई०एस०ओ० बनाये जायें उक्त के साथ ही तकनीकी रूप से दक्ष डिप्टी सी०आई०एस०ओ० (Deputy CISO) भी बनाया जाए। प्रत्येक विभाग में बनाये गये सी०आई०एस०ओ० / डिप्टी सी०आई०एस०ओ० (Deputy CISO) को स्टेट सी०आई०एस०ओ० द्वारा प्रशिक्षित किया जाए।

(कार्यवाही- समस्त विभाग, उ०प्र० शासन तथा आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र०)

1/541141/2024

(7) प्रदेश में साइबर सुरक्षा के दृष्टिगत सीओसीओएमयू (Cyber Crisis Management Unit-CCMS) स्थापित किया जाए एवं विभागवार एसओओपीओ तैयार की जाए जिससे आपात साइबर अटैक आदि को यथाशीघ्र निष्प्रभावी किया जा सके।

(कार्यवाही- आईओटीओ एवं इलेक्ट्रानिक्स विभाग, उओप्रओ)

(8) प्रदेश में स्टेट साइबर ऑडिट टीम (SAT- Cyber) का निर्माण किया जाय, जिसके द्वारा विभिन्न विभागों द्वारा विकसित ऐपलिकेशन्स, वेबसाइट आदि का समय-समय आकस्मिक व नियमित समयवद्ध आडिट किया जाएगा।

(कार्यवाही- आईओटीओ एवं इलेक्ट्रानिक्स विभाग, उओप्रओ)

(9) माओ उच्च न्यायालय और न्याय विभाग से परामर्श प्राप्त कर साइबर अपराधों के सम्बन्ध में ईओ- एफओआईओआरओ की व्यवस्था स्वीकृत की जाय, जिससे राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (NCRP) की शिकायतों का सुचारु रूप से त्वरित निस्तारण कर पीडित का पैसा रिफण्ड किया जा सके।

(कार्यवाही- आईओटीओ एवं इलेक्ट्रानिक्स विभाग, उओप्रओ तथा गृह एवं गोपन विभाग)

(10) CYBER CRIME PREVENTION AGAINST WOMEN AND CHILDREN (CCPWC) से सम्बन्धित साफ्टवेयर का नवीनीकरण किया जाय। उक्त साफ्टवेयर के नवीनीकरण हेतु अनुमानित धन व्यवस्था रु०- 1.7 करोड़ तदनुसार प्रशासकीय विभाग वित्त विभाग की सहमति से निर्भया निधि से सुनिश्चित करें।

(कार्यवाही-आईओटीओ एवं इलेक्ट्रानिक्स विभाग, उओप्रओ, पुलिस महानिदेशक, उओप्रओ तथा गृह(पुलिस)अनुभाग-

15)

(11) गृह मंत्रालय, भारत सरकार की हेल्पलाइन न०:- 1930 द्वारा अधिकतम फोन कॉल्स ग्रहण करने किये जाने की आवश्यकता है। उक्त हेल्पलाइन व्यवस्था के अपग्रेडेशन के लिए आवश्यक धनराशि रु०- 54 लाख की व्यवस्था समयान्तर्गत सुनिश्चित कराया जाए।

(कार्यवाही- आईओटीओ एवं इलेक्ट्रानिक्स विभाग, उओप्रओ तथा पुलिस महानिदेशक, उओप्रओ)

(12) प्रदेश में साइबर क्राइम की लगातार बढ़ती हुई संख्या के दृष्टिगत प्रदेश स्तर पर सक्षम विवेचनाधिकारी पुलिस सब-इंस्पेक्टर से विवेचना कराये जाने के सम्बन्ध में U/S 78 IT ACT में संशोधन किये जाने के सम्बन्ध में सूचना एवं प्रौद्योगिकी मंत्रालय, भारत सरकार से तदनुसार अनुरोध/ सहमति प्राप्त किये जाने हेतु आईओटीओ एवं इलेक्ट्रानिक्स विभाग, उओप्रओ के माध्यम से पुलिस महानिदेशक, साइबर क्राइम आवश्यक कार्यवाही सुनिश्चित करायी जाए।

(कार्यवाही- पुलिस महानिदेशक, उओप्रओ एवं पुलिस महानिदेशक, साइबर क्राइम, उओप्रओ, गृह एवं गोपन विभाग)

(13) साइबर फ्रॉड के माध्यम से विभिन्न पीडित व्यक्तियों का एक खाते में अन्तरित धनराशि बैंकों द्वारा होल्ड करने में होने वाले विलम्ब से साइबर अपराधी द्वारा अन्तरित धनराशि का कुछ भाग अथवा अधिकांश भाग बैंकिंग परिक्षेत्र से बाहर भेज दिया जाता है। शेष जवत् धनराशि को पीडितों के मध्य किस अनुपात में वितरित किया जाये इस सम्बन्ध में एक स्पष्ट नीति बनाये जाने की आवश्यकता है, जिससे होल्ड की गयी धनराशि पीडितों के मध्य अनुपातिक वितरण किया जा सके।

(कार्यवाही- पुलिस महानिदेशक, उओप्रओ एवं पुलिस महानिदेशक, साइबर क्राइम, उओप्रओ)

(14) साइबर सुरक्षा को मजबूत किये जाने एवं साइबर अपराधों पर प्रभावी अंकुश लगाये जाने हेतु व्यापक जन-जागरूकता एवं वित्तीय-साक्षरता बढ़ाये जाने के सम्बन्ध में साइबर सुरक्षा एवं साइबर अपराध के विषय को सम्बन्धित विभाग/संस्थाओं से समन्वय स्थापित कर कक्षा-6 से कक्षा-12 तक के पाठ्यक्रमों में सम्मिलित किया जाए।

-1/541141/2024

(कार्यवाही- माध्यमिक शिक्षा विभाग, क्षेत्रीय मुख्यालय रिजर्व बैंक ऑफ इण्डिया, लखनऊ एवं पुलिस महानिदेशक, साइबर क्राइम, 30प्र0)

(15) साइबर सुरक्षा को मजबूत करने हेतु प्रदेश के प्रत्येक जनपद स्थित साइबर थानों पर तैनात इच्छुक उपनिरीक्षकों को साइबर कमाण्डोज के रूप में प्रशिक्षित कराया जाए। इसके लिए प्रति वर्ष प्रति जनपद 02 प्रतिभागी प्रशिक्षित किये जायेंगे जिसमें 150-150 के दो बैच संचालित किये जायेंगे।

(कार्यवाही- पुलिस महानिदेशक, 30प्र0 तथा पुलिस महानिदेशक, साइबर क्राइम, 30प्र0)

(16) साइबर फ्रॉड से सम्बन्धित शिकायतों पर त्वरित कार्यवाही सुनिश्चित कराये जाने हेतु बैंकों के नोडल अधिकारियों द्वारा साइबर क्राइम से सम्बन्धित शिकायतों का निस्तारण 24X7 सुनिश्चित कराया जाए, जिससे बैंको द्वारा फ्रॉड धनराशि का अन्तरण बैंकिंग परिक्षेत्र से बाहर जाने से पूर्व उक्त धनराशि को फ्रीज/होल्ड समयान्तर्गत किया जा सके।

(कार्यवाही- पुलिस महानिदेशक, साइबर क्राइम, 30प्र0 एवं क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, लखनऊ)

(17) वित्तीय अनियमितताओं/ साइबर अपराध से सम्बन्धित प्रकरणों पर विचार-विमर्श किये जाने हेतु गठित राज्य स्तरीय समन्वय समिति (SECC) की बैठक समय-समय पर सुनिश्चित करायी जाए।

(कार्यवाही- SLCC Convenor RBI एवं क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, कानपुर)

(18) राज्य स्तर पर गहन विश्लेषण ईकाई (यथा I4C में कार्यरत Threat Analytics Units) का गठन कर नागरिकों को सामान्यतया प्राप्त हो रहे एस०एम०एस०, ई.मेल, वॉट्स कॉन्स, अन्य संदेशों, आदि का सुव्यवस्थित संकलन करते हुए सम्भावित साइबर खतरों के विषय में पूर्वानुमान लगाकर बड़ी साइबर त्रासदी को रोकने हेतु कारगर कदम उठाया जाय।

(कार्यवाही- पुलिस महानिदेशक, 30प्र0, पुलिस महानिदेशक, साइबर क्राइम, 30प्र0)

वैठक सधन्यवाद सम्पन्न हुई।

Digitally Signed by दीपक

कुमार

Date: 13-04-2024 19:33:19

Reason: Approved

(दीपक कुमार)

अपर मुख्य सचिव।

उत्तर प्रदेश शासन,

गृह(गोपन) अनुभाग-8

लखनऊ: दिनांक: 15 अप्रैल, 2024

संख्या एवं दिनांक तदैय।

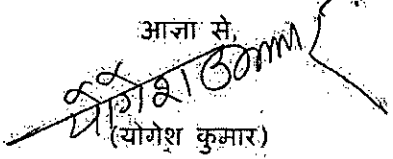
प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

- 1- श्री प्रशान्त कुमार, पुलिस महानिदेशक, 30प्र0।
- 2- श्री नवीन अरोड़ा, अपर पुलिस महानिदेशक, तकनीकी सेवायें, 30प्र0।
- 3- श्री संजीव गुप्ता, सचिव, गृह एवं गोपन विभाग, 30प्र0 शासन।
- 4- श्री अनुराग यादव, सचिव, नियोजन विभाग, 30प्र0 शासन।

1/541141/2024

- 5- श्री ए.वी. राजामौलि, सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
- 6- श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ०प्र०।
- 7- श्री योगेश कुमार, विशेष सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
- 8- श्रीमती नेहा जैन, विशेष सचिव, आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उ०प्र० शासन।
- 9- श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ०प्र०।
- 10- श्रीमती रूपा एम० निदेशक, I4C
- 11- निजी सचिव, मुख्य सचिव, उ०प्र० शासन।
- 12- निजी सचिव, अपर मुख्य सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
- 13- निजी सचिव, अपर मुख्य सचिव, बेसिक शिक्षा विभाग, उ०प्र० शासन।
- 14- निजी सचिव, अपर मुख्य सचिव, वित्त विभाग, उ०प्र० शासन।
- 15- निजी सचिव, अपर मुख्य सचिव, माध्यमिक शिक्षा विभाग, उ०प्र० शासन।
- 16- क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, लखनऊ।
- 17- क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, कानपुर।
- 18- गृह (पुलिस) अनुभाग-9
- 19- गृह (पुलिस) अनुभाग-15

आज्ञा से,



(योगेश कुमार)

विशेष सचिव ।