सरकारी कर्मचारियों
के लिए
साइबर सुरक्षा दिशानिर्देश

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय

एनआईसी
National Informatics Centre

ए-ब्लॉक, सीजीओ कॉम्प्लेक्स
नई दिल्ली - 110003
वेबसाइट: https://www.nic.in/

दस्तावेज़ नियंत्रण

दस्तावेज़ का नाम: सरकारी कर्मचारियों के लिए साइबर सुरक्षा दिशानिर्देश
दस्तावेज़ आईडी संदर्भ: सीजीजीई

प्राधिकरण:

क्रमांक	नाम	पदनाम	भूमिका
1	श्री अलकेश कुमार शर्मा	सचिव , एमईआईटीवाई	अनुमोदन प्राधिकारी
2	डॉ राजेंद्र कुमार	एएस , एमईआईटीवाई	समीक्षक
3	श्री राजेश गेरा	डीजी, एनआईसी	समीक्षक
4	डॉ. संजय बहल	डीजी, (CERT-IN)	समीक्षक
5	श्री आर.एस. मणि	डीडीजी, एनआईसी	समीक्षक
6	श्री सी.जे. एंटनी	डीडीजी, एनआईसी	समीक्षक
7	डॉ. सीमा खन्ना	डीडीजी, एनआईसी	समीक्षक
8	श्री एस.एस. शर्मा	वैज्ञानिक-एफ, (CERT-IN)	समीक्षक
9	श्री हरि हरन	एस एस ए एनआईसी	लेखक

सुरक्षा वर्गीकरण: प्रतिबंधित

संस्करण इतिहास:

जारी करने की तिथि	प्रभावी तिथि	विवरण
1.1	7-जून-2022	ड्राफ्ट - ,अनुभाग 5(साइबर सुरक्षा संसाधन) जोड़ा गया	
1.2	8-जून-2022	ड्राफ्ट - सीईआरटी-इन से इनपुट जोड़े गए और DNS सर्वर IPv4 और IPv6 IP पते को शामिल किया गया|
1.3	10-जून-2022	अंतिम रिलीज़ (संस्करण)	

वितरण सूची:

निम्नलिखित व्यक्ति / संस्थानों के पास दस्तावेजों की प्रतियां होगी। दस्तावेजो में होने वाले सभी संशोधन और अद्यतन सूचनाएं वितरण सूचि के अनुसार वितरित किए जाने चाहिए।

क्रमांक	नाम	स्थान	दस्तावेज़ प्रकार
1	सरकारी मंत्रालय और विभागों	भारत भर में	सॉफ्ट कॉपी

गोपनीयता

इस दस्तावेज़ में राष्ट्रीय सूचना विज्ञान केंद्र से संबंधित प्रतिबंधित जानकारियां है। दस्तावेज़ के लिए पहुँच गोपनीय स्तर का है। सभी के द्वारा पहुंच के स्तर पर गोपनीयता का सम्मान अपेक्षित है।

अस्वीकरण:

यह दस्तावेज़ केवल सरकारी कर्मचारियों और आउटसोर्स/संविदात्मक संसाधनों की जानकारी के लिए है और NIC/MeitY की पूर्व लिखित सहमति के बिना इसे किसी अन्य उद्देश्य के लिए उपयोग, परिचालित, उद्धृत या अन्यथा संदर्भित नहीं किया जाना चाहिए और न ही किसी दस्तावेज़ में पूर्ण या आंशिक रूप से शामिल या संदर्भित किया जाना चाहिए।

विषयसूची

1 परिचय.. 5

2 साइबर सुरक्षा क्या करें 5

3 साइबर सुरक्षा - क्या न करें 8

4 साइबर सुरक्षा संसाधन 10

5 अनुपालन 11

1 परिचय

देश भर के सरकारी मंत्रालयों और विभागों में सूचना और संचार प्रौद्योगिकी (आईसीटी) का उपयोग सर्वव्यापी हो गया है। आईसीटी को अपनाने में बढ़ोत्तरी होने और इसके बढ़ते हुए उपयोग ने सरकार के लिए साइबर हमले की सम्भावना और उससे होने वाले खतरे की धारणा को बढ़ा दिया है। क्योंकि व्यवहार में अपनाई जाने वाली साइबर सुरक्षा प्रथाओं में कमी है। सरकारी कर्मचारियों और संविदा/आउटसोर्स संसाधनों को संवेदनशील बनाने और साइबर सुरक्षा के दृष्टिकोण से क्या करना है और क्या नहीं करना है, इस बारे में उनके बीच जागरूकता पैदा करने के लिए, इन दिशानिर्देशों को संकलित किया गया है। देशभर के सरकारी कार्यालयों में समान साइबर सुरक्षा दिशानिर्देशों का पालन करके सरकार की सुरक्षा स्थिति में सुधार किया जा सकता है।

2 साइबर सुरक्षा- क्या करें

1. बड़े अक्षरों, छोटे अक्षरों, संख्याओं और विशेष वर्णों के संयोजन का उपयोग करके कम से कम 8 वर्णों वाले जटिल पासवर्ड का उपयोग करें।

2. 45 दिनों में कम से कम एक बार अपना पासवर्ड बदलें।

3. जहां कहीं भी उपलब्ध हो, बहु-कारक प्रमाणीकरण का उपयोग करें। (जैसे पासवर्ड और मोबाइल पर ओ.टी.पी.)

4. अपने डेटा और फाइलों को कम्प्यूटर की सेकेंडरी ड्राइव पर सेव करें (उदा: d:\)।

5. अपने महत्वपूर्ण डेटा का ऑफ़लाइन बैकअप बनाए रखें।

6. अपने ऑपरेटिंग सिस्टम और (BIOS FIRMWARE) को नवीनतम अपडेट/पैच के साथ अपडेट रखें।

7. अपने आधिकारिक डेस्कटॉप/लैपटॉप पर सरकार द्वारा प्रस्तावित इंटरप्राइज़ एंटीवायरस क्लाइंट इंस्टॉल करें। सुनिश्चित करें कि एंटीवायरस क्लाइंट नवीनतम वायरस परिभाषाओं, हस्ताक्षरों और पैच के साथ अद्यतन है।

8. अपने सिस्टम की DNS सेटिंग्स में NIC के DNS सर्वर IP (IPv4: 1.10.10.10/ IPV6: 2409::1) को कॉन्फिगर करें।

9. समय सिंक्रोनाइज़ेशन (Time Synchronization) के लिए अपने सिस्टम की एनटीपी सेटिंग्स में एनआईसी की एनटीपी सेवा (samay1.nic.in, samay2.nic.in) को कॉन्फिगर करें।

10. अधिकृत और लाइसेंस प्राप्त सॉफ्टवेयर का ही प्रयोग करें।

11. सुनिश्चित करें कि कम्प्यूटर / सिस्टम पर उचित (Security Hardening) सुनिश्चित की गई है|

12. जब आप अपनी डेस्क को अस्थायी रूप से छोड़ते हैं तो अपने कंप्यूटर सत्र से हमेशा लॉग-ऑफ करें अथवा इसे लॉक करे ।

13. जब आप कार्यालय छोड़ते हैं, तो सुनिश्चित करें कि आपका कंप्यूटर और प्रिंटर ठीक से शटडाउन है।

14. अपने प्रिंटर के सॉफ्टवेयर को नवीनतम अपडेट/पैच से अपडेट रखें।

15. साझा प्रिंटर के लिए अद्वितीय (Unique) पासकोड सेट करें।

16. डेटा केंद्रों में स्थित किसी भी आईटी सिस्टम से निजी तौर पर कनेक्ट करने के लिए हार्डवेयर वर्चुअल प्राइवेट नेटवर्क (वीपीएन) टोकन का उपयोग करें।

17. अपने कंप्यूटर और मोबाइल फोन पर GPS, ब्लूटूथ, NFC और अन्य सेंसर बंद रखें, आवश्यकता पड़ने पर ही इन्हें चालू करें।

18. गूगल (एंड्रायड के लिए) और एप्पल (आईओएस के लिए) के आधिकारिक ऐप स्टोर से ही ऐप डाउनलोड करें ।

19. ऐप डाउनलोड करने से पहले ऐप की लोकप्रियता की जांच करें और उपयोगकर्ताओ की समीक्षा को पढ़ें । खराब प्रतिष्ठा या कम उपयोगकर्ताओ वाले ऐप डाउनलोड करने से बचें एवं सावधानी बरतें।

20. नियमित काम के लिए अपने कंप्यूटर/लैपटॉप तक पहुंचने के लिए नॉन -एडमिनिस्ट्रेटर खाते का उपयोग करें।

21. इलेक्ट्रॉनिक माध्यम से कोई भी महत्वपूर्ण सूचना या दस्तावेज भेजते समय, कृपया ट्रांसमिशन से पहले डेटा को इंक्रिप्ट करें। आप एक लाइसेंस प्राप्त एन्क्रिप्शन सॉफ्टवेयर अथवा ओपन पीजीपी आधारित इन्क्रिप्शन सॉफ्टवेयर का उपयोग कर सकते हैं । फाइलों को एक Compressed ZIP File में जोड़ें और जिप को पासवर्ड से सुरक्षित रखें। संरक्षित फाइलों को खोलने के लिए पासवर्ड को किसी दूसरे संचार माध्यम जैसे एसएमएस, सन्देश आदि के माध्यम से प्राप्तकर्ता के साथ साझा किया जाना चाहिए।

22. कोई छोटा यूनिफॉर्म रिसोर्स लोकेटर (यूआरएल) खोलते समय सावधानी बरतें (उदाहरण: tinyurl.com/ab534/)। कई मालवेयर और फिशिंग साइटें (यूआरएल) शॉर्टनर सेवाओं का दुरुपयोग करती हैं।

23. एसएमएस या सोशल मीडिया आदि के माध्यम से साझा किए गए किसी भी लिंक को खोलते समय सावधानी बरतें, जहां लिंक रोमांचक ऑफर / छूट या किसी भी करंट अफेयर्स के बारे में विवरण प्रदान करने का दावा करते हों । ऐसा लिंक फिशिंग / मैलवेयर वेबपेज पर ले जा सकता हैं, और आपके डिवाइस की सुरक्षा से समझौता कर सकता है।

24. संदेहास्पद ईमेल या किसी भी सुरक्षा घटना की सूचना incident@cert-in.org.in और incident@nic-cert.nic.in पर दें।

25. एनआईसी-सीईआरटी (https://niccert.nic.in/advisories.jsp) और सीईआरटी-इन (https://www.cert-in.org.in) द्वारा प्रकाशित सुरक्षा परामर्शों का पालन करें।

3 साइबर सुरक्षा - क्या न करें

1. एक से अधिक सेवाओं / वेबसाइटों/ऐप्स में एक ही पासवर्ड का उपयोग न करें।

2. अपने पासवर्ड को ब्राउजर में या किसी भी असुरक्षित दस्तावेज में सुरक्षित (save) न करें।

3. किसी भी असुरक्षित वस्तु पर कोई पासवर्ड, आईपी एड्रेस, नेटवर्क डायग्राम या अन्य संवेदनशील जानकारी न लिखें उदाहरण:- स्टिक लेबल, नोट्स, सादे कागज, आपकी टेबल पर पड़े कागज आदि।

4. अपने डेटा और फाइलों को सिस्टम ड्राइव पर सेव न करें (उदाहरण: c:\ या root \) ।

5. किसी भी गैर-सरकारी क्लाउड सेवा (उदाहरण: गूगल ड्राइव, ड्रॉपबॉक्स, आदि) पर किसी भी आंतरिक / प्रतिबंधित / गोपनीय सरकारी डेटा या फाइलों को अपलोड या सेव न करें।

6. अप्रचलित, पुराने या आउट-डेटेड ऑपरेटिंग सिस्टम का उपयोग न करें।

7. किसी भी तृतीय पक्ष DNS सेवा या NTP सेवा का उपयोग न करें।

8. किसी भी तृतीय पक्ष गुमनाम करने वाली सेवाओं (anonymization services) (उदाहरण: नॉर्ड वीपीएन, एक्सप्रेस वीपीएन, टोर (TOR), प्रॉक्सी, आदि) का उपयोग न करें।

9. अपने इंटरनेट ब्राउज़र में किसी भी तृतीय पक्ष टूलबार (उदाहरण: डाउनलोड प्रबंधक (Download Manager), मौसम टूल (Weather Tool) बार, Ask Me, टूल बार, आदि) का उपयोग न करें।

10. किसी भी पायरेटेड सॉफ्टवेयर को स्थापित या उपयोग न करें (उदाहरण: cracks, keygen, आदि)।

11. **किसी अज्ञात प्रेषक द्वारा भेजे गए ईमेल में निहित किसी भी लिंक या अटैचमेंट को न खोलें।**

12. सिस्टम पासवर्ड या प्रिंटर पासकोड या वाई-फाई पासवर्ड किसी भी अनधिकृत व्यक्ति के साथ साझा न करें।

13. प्रिंटर को इंटरनेट एक्सेस की अनुमति न दें।

14.प्रिंटर को अपने प्रिंट इतिहास को स्टोर करने की अनुमति न दें।

15.सोशल मीडिया या तीसरे पक्ष के मैसेजिंग ऐप पर किसी भी संवेदनशील विवरण का खुलासा न करें।

16.किसी अज्ञात व्यक्ति द्वारा साझा की गई यूएसबी ड्राइव सहित किसी भी अनधिकृत बाहरी डिवाइस को प्लग-इन न करें।

17. किसी भी अनधिकृत रिमोट एडमिनिस्ट्रेशन टूल का उपयोग न करें (उदाहरण: Teamviewer, Ammy admin, anydesk, आदि)

18. संवेदनशील आंतरिक बैठकों और चर्चाओं के संचालन के लिए किसी भी अनधिकृत तृतीय पक्ष वीडियो कॉन्फ्रेंसिंग प्रणाली या संसाधनों का उपयोग न करें।

19. आधिकारिक संचार के लिए किसी बाहरी ईमेल सेवा का उपयोग न करें।

20. अपने मोबाइल फोन को जेलब्रेक या रूट न करें।

21. अपने नियमित कार्य के लिए एडमिनिस्ट्रेटर खाते या प्रशासनिक विशेषाधिकार वाले किसी अन्य खाते का उपयोग न करें।

22. आंतरिक सरकारी दस्तावेजों को स्कैन करने के लिए किसी बाहरी मोबाइल ऐप आधारित स्कैनर सेवाओं (उदाहरण: कैमस्कैनर आदि) का उपयोग न करें।

23. किसी सरकारी दस्तावेज़ को परिवर्तित/ कम्प्रेस करने के लिए किसी बाहरी वेबसाइट या क्लाउड-आधारित सेवाओं का उपयोग न करें (उदाहरण: वर्ड टू पीडीएफ या फाइल साइज कम्प्रेशन)

24. **कोई भी संवेदनशील जानकारी किसी अनधिकृत या अज्ञात व्यक्ति के साथ टेलीफोन पर या किसी अन्य माध्यम से साझा न करें।**

4 साइबर सुरक्षा संसाधन

साइबर सुरक्षा के बारे में अधिक जानकारी के लिए निम्नलिखित संसाधनों को संदर्भित किया जा सकता है:

क्रमांक	संसाधन यूआरएल	विवरण
1	https://www.meity.gov.in/cybersecurity-division	कानून, नीतियां और दिशानिर्देश
2	https://www.cert-in.org.in	सुरक्षा सलाह, दिशानिर्देश और अलर्ट
3	https://nic-cert.nic.in	सुरक्षा सलाह, दिशानिर्देश और अलर्ट
4	https://www.csk.gov.in	सुरक्षा उपकरण और सर्वोत्तम अभ्यास
5	https://infosecawareness.in	सुरक्षा जागरूकता सामग्री
6	http://cybercrime.gov.in	साइबर अपराध की रिपोर्ट साइबर,सुरक्षा युक्तियाँ

5 अनुपालन

अस्थायी, संविदा/आउटसोर्स संसाधनों सहित सभी सरकारी कर्मचारियों को इस दस्तावेज़ में उल्लिखित दिशानिर्देशों का कड़ाई से पालन करना आवश्यक है। गैर-अनुपालन पर संबंधित सीआईएसओ (CISO - मुख्य सूचना सुरक्षा अधिकारी) /विभाग प्रमुखों द्वारा कार्रवाई की जा सकती है।