सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

NCVET
कौशल गुणवत्ता प्रगति

सूचना और डेटा सुरक्षा के लिए दिशानिर्देश

राष्ट्रीय व्यावसायिक शिक्षा और प्रशिक्षण परिषद् (एनसीवीईटी)

फा. सं. 22001/02/2024/एनसीवीईटी दिनांकः 27.05.2024

विषय : सूचना और डेटा सुरक्षा के लिए दिशानिर्देश

1. आज के डिजिटल युग में, जहां पर सूचना लगातार प्रवाहित हो रही है और डेटा संगठनों के संचालन का मूल आधार है, अतः संवेदनशील सूचना की सुरक्षा अत्यंत महत्वपूर्ण है। सूचना और डेटा सुरक्षा में ऐसे व्यापक सिद्धांत, पद्धतियां और प्रौद्योगिकियां शामिल हैं, जिनसे कि डेटा को अनधिकृत पहुंच, प्रकटन, हेराफेरी और उन्हें नष्ट किए जाने से बचाया जा सके। इसमें चाहे वह वित्तीय रिकार्ड हो, ग्राहक सूचना हो, बौद्धिक संपत्ति हो या स्वामित्व के व्यवसाय संबंधी डेटा हो, उसका हर हिस्सा महत्वपूर्ण होता है और उसकी सुरक्षा आवश्यक होती है।

2. एनसीवीईटी के लिए सूचना और डेटा सुरक्षा व्यावसायिक शिक्षा, प्रशिक्षण और कौशल (वीईटीएस) के विकास, गुणवत्तापरक सुधार और विनियमन के संदर्भ में महत्वपूर्ण भूमिका के कारण बहुत ही महत्वपूर्ण है। एनसीवीईटी के नियंत्रण में अत्यधिक संवेदनशील डेटा की प्रामाणिकता और गोपनीयता की सुरक्षा अत्यावश्यक है।

3. अतः एनसीवीईटी ने सूचना और डेटा सुरक्षा के संबंध में दिशानिर्देश तैयार किया हैं। इस दिशानिर्देश से कर्मचारियों की व्यक्तिगत सूचना और व्यावसायिक प्रशिक्षण, मूल्यांकन परिणाम, मान्यता के ब्यौरे और विभिन्न अन्य गोपनीय रिकार्ड रखने वाले व्यक्तियों की निजी सूचना की सुरक्षा का समाधान होगा। इसके साथ ही, शैक्षणिक और प्रशिक्षण प्रक्रियाओं के बढ़ते डिजिटाइजेशन को देखते हुए, मजबूत "सूचना और डेटा सुरक्षा" के उपाय करना आवश्यक है ताकि डेटा की चोरी, अनधिकृत पहुंच और ऐसे साइबर खतरों से सुरक्षा हो सके, जिसके कारण एनसीवीईटी की देखरेख वाले क्रियाकलापों में विश्वास और प्रभावकारिता के साथ समझौता होता हो।

4. इस दिशानिर्देश में एनसीवीईटी के लिए अनिवार्य न्यूनतम सूचना सुरक्षा अपेक्षाओं को परिभाषित किया गया है। कोई संस्था (जैसे अवार्डिंग निकाय और मूल्यांकन एजेंसियां), एनसीवीईटी के साथ जुड़कर अपनी व्यक्तिगत कारोबारी जरूरतों और विशिष्ट कानूनी तथा संघीय अपेक्षाओं के आधार पर दिशानिर्देश में दी गई सुरक्षा अपेक्षाओं से आगे बढ़ सकती है लेकिन उसे कम से कम इस दिशानिर्देश में उल्लिखित सुरक्षा स्तरों को प्राप्त करना होगा।

5. एनसीवीईटी की दिनांक 21 फरवरी, 2024 को आयोजित 10वीं परिषद् बैठक में दिशानिर्देश को प्रस्तुत किया गया था और इसे एतदद्वारा अधिसूचित किया जा रहा है। इस दिशानिर्देश के कार्यान्वयन के दौरान प्राप्त फीडबैक और अपेक्षाओं के आधार पर इस दिशानिर्देश में एनसीवीईटी के अनुमोदन से समय-समय पर आगे संशोधन/ अद्यतन किया जा सकता हैं।

(डॉ. सुहास देशमुख)
निदेशक, एनसीवीईटी

आमुख

निरंतर विकसित हो रहे डिजिटल परिदृश्य में, सूचना और डेटा सुरक्षा को सुरक्षित रखना सर्वोच्च प्राथमिकता है। चूंकि हम एक ऐसे युग से होकर गुजर रहे हैं, जहां डेटा निरंतर प्रवाहित होता रहता है और यह दुनिया भर में संगठनों के मुख्य संचालन का आधार है, अत: ऐसी संवेदनशील सूचना को डिजिटल युग में मौजूद असंख्य भेद्यताओं से बचाना अनिवार्य हो जाता है।

राष्ट्रीय व्यावसायिक शिक्षा और प्रशिक्षण परिषद् (एनसीवीईटी) पूरे देश में व्यावसायिक शिक्षा, प्रशिक्षण और कौशल (वीईटीएस) व्यवस्था और विभिन्न कौशल पहलों के नियमन में एक महत्वपूर्ण भूमिका निभाती है। एनसीवीईटी द्वारा प्रबंधित डेटा अत्यंत महत्वपूर्ण और संवेदनशील है, जिसमें कर्मचारियों की व्यक्तिगत सूचना, व्यावसायिक प्रशिक्षण प्राप्त करने वाले व्यक्तियों का ब्यौरा, मूल्यांकन के परिणाम और मान्यता/प्रत्यायन रिकार्ड एवं अन्य महत्वपूर्ण डेटा सम्मिलित है। परिणामस्वरूप एनसीवीईटी की इस सूचना की सटीकता, प्रामाणिकता और सुरक्षा के रखरखाव में महत्वपूर्ण जिम्मेदारी है।

इन उत्तरदायित्वों की गहन जानकारी के साथ, एनसीवीईटी ने सूचना और डेटा सुरक्षा के लिए ठोस दिशानिर्देश तैयार करने की शुरुआत की है। ये दिशानिर्देश बड़े परिश्रम से तैयार किए गए हैं, ताकि आईएसओ 27001 मानकों की अनुपालना और राष्ट्रीय साइबर सुरक्षा नीति, 2013 और डिजिटल निजी डेटा संरक्षण अधिनियम, 2023 (डीपीडीपीए) की व्यवस्थाओं की अनुपालना सुनिश्चित हो सके। सूचना और डेटा सुरक्षा का सक्रियतापूर्वक समाधान करके, एनसीवीईटी ने उसे सौंपी गई संवेदनशील सूचना की सुरक्षा के लिए अपना अटूट समर्पण प्रदर्शित किया है। यह कार्यनीतिक दृष्टिकोण सुनिश्चित करता है कि वीईटीएस पहल एक सुरक्षित और भरोसेमंद वातावरण में समृद्ध हो सकती है, जिससे व्यक्तियों और संगठनों की अपनी पूर्ण क्षमता प्राप्त करने में सक्षम बनाया जा सकता है।

इस दिशानिर्देश को अति सावधानीपूर्वक प्रक्रिया से विकसित किया गया है। एनसीवीईटी ने व्यापक कानूनी और संघीय मानदंडों की अनुपालना सुनिश्चित करते हुए संगठनात्मक आवश्यकताओं के अनुरुप अपेक्षाएं तैयार करने के लिए राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) की टीम के साथ मिलकर काम किया है। कर्मयोगी भारत द्वारा प्रदान की गई व्यवस्था से प्रेरित होकर और विभिन्न हितधारकों के साथ निरंतर परामर्श करके, एक प्रारूप पर विचार किया गया और बाद में उसे जनता की जानकारी के लिए रखा गया था। यह परामर्शी कार्य विविध

दृष्टिकोणों और जानकारियों के साथ दिशानिर्देश तैयार करने में महत्वपूर्ण था, जिससे उनकी प्रासंगिकता और प्रयोज्यता बढ़ी।

मैं सभी हितधारकों के प्रति अपना हार्दिक आभार प्रकट करता हूं, जिन्होंने परामर्श प्रक्रिया में सक्रिय रूप से भाग लिया और इस व्यापक नीतिगत दस्तावेज को तैयार करने के लिए अपना महत्वपूर्ण योगदान दिया। इस कार्यनीतिक दिशानिर्देश से व्यावसायिक शिक्षा, प्रशिक्षण और कौशल (वीईटीएस) समुदाय को सशक्त बनाया जा सकेगा, जिससे उनकी सूचना सुरक्षा की स्थिति मजबूत होगी और उन्हें प्रदान किए गए संवेदनशील डेटा की सुरक्षा होगी। इन सशक्त मानकों का अनुपालन होने से, संगठन में एक भरोसेमंद वातावरण का निर्माण होगा, जिससे व्यक्ति और उद्यम सफलता की नई ऊंचाइयों पर पहुंचने में समर्थ होंगे।

मैं सभी हितधारकों व सरकारी एजेंसियों, अवार्डिंग निकायों, मूल्यांकन एजेंसियों और व्यापक वीईटीएस समुदाय से आग्रह करता हूं कि "सूचना और डेटा सुरक्षा के लिए दिशानिर्देश" लागू करें। इस तरह से हम हितधारकों के डेटा, कौशल व्यवस्था के भविष्य को सुरक्षित कर सकते हैं और राष्ट्र के श्रम बल को सशक्त बना सकते हैं ताकि ये इस डिजिटल युग में समृद्ध हो सकें।

मैं एनसीवीईटी में कार्यकारी सदस्यों, डॉ. नीना पाहुजा और डॉ. विनीता अग्रवाल के कुशल मार्गदर्शन में डॉ. सुहास देशमुख, निदेशक, श्री प्रदीप थोटा, उप निदेशक, श्री अमरेश कुमार, सलाहकार और सुश्री रत्ना प्रिया कंचन, युवा पेशेवर सहित एनसीवीईटी टीम के द्वारा किए गए कार्य के लिए भी आभार प्रकट करता है। एनसीवीईटी को एमएसडीई, राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी), कर्मयोगी भारत और अन्य प्रतिष्ठित संगठनों से इस दिशानिर्देश को तैयार करने के लिए बहुमूल्य जानकारी भी प्राप्त हुई, जिनके लिए मैं हार्दिक आभार प्रकट करता हूं। एनसीवीईटी गतिशील प्रकृति के इस दिशानिर्देश में सुधार के लिए अन्य सुझावों का स्वागत करता है, और इसे आवधिक रूप से अद्यतन किया जाएगा।

"सूचना और डेटा सुरक्षा के लिए दिशानिर्देश" के कार्यान्वयन के लिए मेरी शुभकामनाएं।

डॉ. एन.एस. कलसी,
आईएएस, सेवानिवृत्त
अध्यक्ष, एनसीवीईटी

विषय सूची

1. प्रस्तावना

राष्ट्रीय व्यावसायिक शिक्षा और प्रशिक्षण परिषद् (एनसीवीईटी) को पूर्ववर्ती राष्ट्रीय कौशल विकास एजेंसी (एनएसडीए) और राष्ट्रीय व्यावसायिक प्रशिक्षण परिषद् (एनसीवीटी) का विलय करके सरकार द्वारा दिनांक 5 दिसंबर, 2018 को अधिसूचना सं. एसडी-17/113/2017-ई एंड पी डब्ल्यू के तहत अधिसूचित किया गया है। एनसीवीईटी की स्थापना होने से व्यावसायिक शिक्षा और प्रशिक्षण (वीईटी) तथा कौशल पारिस्थितिकी तंत्र में अलग-अलग नियामक ढांचे को भी समेकित किया गया है।

राष्ट्रीय व्यावसायिक शिक्षा और प्रशिक्षण परिषद् को अवार्डिंग निकायों, मूल्यांकन एजेंसियों, कौशल सूचना प्रदाताओं और प्रशिक्षण निकायों के कार्यकरण को मान्यता प्रदान करने और निगरानी रखने तथा अधिसूचना में यथानिर्दिष्ट अन्य प्रासंगिक कार्यों का निष्पादन करने के लिए व्यावसायिक शिक्षा और प्रशिक्षण के विकास, गुणवत्तापरक सुधार और नियमन का कार्य सौंपा गया है।

व्यावसायिक शिक्षा, प्रशिक्षण और कौशल विकास (वीईटी एवं एसडी) के विकास, गुणवतापरक सुधार और नियमन की निगरानी में भूमिका के कारण एनसीवीईटी के लिए सूचना और डेटा सुरक्षा अत्यंत महत्वपूर्ण है एनसीवीईटी के नियंत्रण वाले भारी मात्रा में संवेदनशील डेटा की प्रामाणिकता और गोपनीयता की सुरक्षा करना महत्वपूर्ण है। इसमें कर्मचारियों और व्यावसायिक प्रशिक्षण प्राप्त कर रहे व्यक्तियों की निजी सूचना, मूल्यांकन के परिणाम, प्रत्यायन के ब्यौरे और विभिन्न अन्य गोपनीय रिकार्ड शामिल है। इसके अलावा शिक्षा और प्रशिक्षण प्रक्रियाओं के बढ़ते डिजिटलीकरण को ध्यान में रखते हुए, मजबूत "सूचना और डेटा सुरक्षा" उपायों को सुनिश्चित करना आवश्यक है, ताकि डेटा की चोरी, अनधिकृत पहुंच और साइबर हमलों को रोका जा सके, जो एनसीवीईटी की निगरानी वाले क्रियाकलापों के भरोसे और प्रभावकारिता से समझौता कर सकते हैं। अतः हितधारकों के विश्वास को बनाए रखने, संवेदनशील डेटा के संरक्षण के लिए और वीईटीएस का सुचारू व सुरक्षित कार्यक्रम सुनिश्चित करने के लिए एनसीवीईटी के लिए एक मजबूत "सूचना और डेटा सुरक्षा फ्रेमवर्क" अनिवार्य है।

2. नीति का प्रयोजन

यह नीति एनसीवीईटी के लिए न्यूनतम सूचना सुरक्षा की श्रेष्ठ प्रक्रियाओं को परिभाषित करती है, जैसा कि नीचे कार्यक्षेत्र खंड में दिया गया है। एनसीवीईटी से संबद्ध किसी भी संस्था के

लिए यह अनिवार्य है कि वह नीति द्वारा अपेक्षित सुरक्षा स्तरों का पालन करे। यद्यपि उन्हें अपनी व्यक्तिगत कारोबारी जरूरतों और कानूनी बाध्यताओं के आधार पर इन अपेक्षाओं से परे छूट है, लेकिन दस्तावेज में उल्लिखित न्यूनतम सुरक्षा स्तरों को पूरा करना अनिवार्य है।

यह नीति सभी अन्य सुरक्षा नीतियों और संबद्ध मानकों के लिए एक व्यापक दस्तावेज के रूप में कार्य करती है। यह नीति निम्नलिखित कार्यविधियां पूरी करती है :

- सूचना और संगत अवसंरचना परिसंपत्तियों की गोपनीयता, प्रामाणिकता और उपलब्धता का संरक्षण और रखरखाव करना;
- सुरक्षा प्रकटन अथवा समझौते के जोखिम का प्रबंधन करना;
- एक सुरक्षित और स्थायी सूचना प्रौद्योगिकी (आईटी) परिवेश सुनिश्चित करना;
- सूचना परिसंपत्ति के दुरुपयोग, हानि अथवा अनधिकृत प्रकटन वाली घटनाओं की पहचान करना और उन पर कार्रवाई करना;
- ऐसी विसंगतियों की निगरानी व्यवस्था करना, जिनसे संकट की स्थिति प्रतीत होती हो; और
- सूचना सुरक्षा की जागरूकता को प्रोत्साहित करना और बढ़ाना।

वर्तमान समय के अत्यधिक नेटवर्क वाले वातावरण में सूचना परिसंपत्तियों की गोपनीयता, प्रामाणिकता और उपलब्धता की सुरक्षा और संरक्षा करने में विफलता से ऐसी प्रणालियों को क्षति हो सकती है या वे बंद हो सकती हैं, जो महत्वपूर्ण अवसंरचना, वित्तीय और कारोबारी सौदों तथा महत्वपूर्ण सरकारी कार्यों का संचालन करती हैं, डेटा संकट में पड़ सकता है; और परिणास्वरूप कानूनी व नियामक अनुपालन नहीं हो पाता।

नीति ऐसा फ्रेमवर्क बनाने में मदद करती है, जिससे ऐसे उपयुक्त उपाय सुनिश्चित किए जाएंगे जिनसे डेटा की गोपनीयता, प्रामाणिकता और उपलब्धता का संरक्षण हो सके। इससे यह भी सुनिश्चित होता है कि स्टॉफ और सभी अन्य संबद्ध संस्थाएं अपने कार्यों और उत्तरदायित्वों को समझें, सुरक्षा नीति, प्रक्रिया और पद्धतियों की पर्याप्त जानकारी रखें और यह जाने कि कैसे सूचना का संरक्षण किया जाए।

3. कार्यक्षेत्र

यह नीति एनसीवीईटी के सभी स्थानों पर, मूल कंपनी के कर्मचारियों, और तदनुरूप एनसीवीईटी के लिए कार्य कर रहे संबद्ध ठेकेदारों/वेंडरों पर लागू है। यह ऐसे प्रयोक्ताओं/शिक्षुओं, बाह्य सेवा

प्रदाताओं और/अथवा अतिथियों से प्राप्त सूचना पर लागू है, जिन्हें एनसीवीईटी द्वारा अप्रकटित सूचना संप्रेषित अथवा उपलब्ध कराई जाती है।

इस नीति में ऑटोमेटेड और मैनुअल सभी प्रणालियां शामिल है, जिनके लिए एनसीवीईटी को जिम्मेदारी दी गई है, जिनमें एनसीवीईटी की ओर से अन्य पक्षों द्वारा प्रबंधित अथवा मेजबानी वाली प्रणालियां शामिल हैं। इसमें सभी सूचनाओं का ध्यान रखा गया है, चाहे वे किसी भी रूप या प्रारूप में हो, जो कारोबारी क्रियाकलापों के समर्थन में सृजित अथवा प्रयुक्त हुई हों।

निम्नलिखित प्रमुख क्षेत्रों को इस दस्तावेज के भाग के रूप में शामिल किया गया है। इन्हें नीचे सूचीबद्ध किया गया है:

1. नेटवर्किंग और अवसंरचना सुरक्षा
2. पहचान, पहुंच और विशेषाधिकार प्रबंधन
3. भौतिक सुरक्षा
4. डेटा सुरक्षा और नियंत्रण
5. खतरा और संवेदनशीलता प्रबंधन
6. निजी सुरक्षा
7. सुरक्षा और दुर्घटना प्रबंधन
8. आईटी परिसंपत्ति प्रबंधन
9. मोबिलिटी और अपना स्वयं का उपकरण लाएं (बीवाईओडी)
10. वर्चुअलाइजेशन
11. सोशल मीडिया
12. सुरक्षा परीक्षण
13. सुरक्षा ऑडिट
14. प्रचालन सुरक्षा

4. सूचना वर्गीकरण दिशानिर्देश

एनसीवीईटी के पास उपलब्ध समस्त सूचना निम्नलिखित श्रेणियों में से किसी एक श्रेणी में वर्गीकृत की जाएगी (गृह मंत्रालय द्वारा जारी कागजात अभिलेख संबंधी मैन्युअल, 1994 के मौजूदा वर्गीकरण पर आधारित):

1. **अति गुप्त :** ऐसी सूचना, जिसका अप्राधिकृत प्रकटन होने से राष्ट्रीय सुरक्षा अथवा राष्ट्रीय हित को असाधारण क्षति होने की संभावना हो। यह श्रेणी राष्ट्र के सर्वाधिक गुप्त के लिए आरक्षित है और इसका अत्याधिक सावधानी से प्रयोग किया जाना चाहिए।

2. **गुप्त :** ऐसी सूचना, जिसका अप्राधिकृत प्रकटन होने से राष्ट्रीय सुरक्षा अथवा राष्ट्रीय हित को नुकसान हो सकता हो अथवा उसके कार्यकरण में गंभीर शर्मिंदगी होने की संभावना हो। इस वर्गीकरण का उपयोग अति महत्वपूर्ण सूचना के लिए किया जाए और यह सामान्यतः प्रयोग किया जाने वाला सर्वोच्च वर्गीकरण है।

3. **गोपनीय :** ऐसी सूचना, जिसका अप्राधिकृत प्रकटन होने से संगठन की सुरक्षा को क्षति होने की संभावना हो अथवा संगठन के हित के लिए हानिकारक हो सकता हो, संगठन के कार्यकरण पर प्रभाव पड़ता हो। अधिकांश सूचना का कागजी विश्लेषण करने पर उन्हें गोपनीय से अधिक वर्गीकरण नहीं दिया जाएगा।

4. **प्रतिबंधित :** ऐसी सूचना, जो अनिवार्य रूप से केवल आधिकारिक प्रयोग के लिए है और जिसे आधिकारिक प्रयोजन के अलावा किसी अन्य को भी प्रकाशित या सूचित नहीं किया जाएगा।

5. **अवर्गीकृत :** ऐसी सूचना, जिसके प्रकटन के लिए कोई संरक्षण अपेक्षित नहीं है अर्थात सार्वजनिक विज्ञप्ति।

सूचना संचालन : एनसीवीईटी द्वारा कर्मचारियों और संगत पक्षों को उनको जानने की आवश्यकता के आधार पर ही सूचना साझा की जाएगी और इस नीति दस्तावेज में यथा परिभाषित समुचित संचार माध्यमों से ही सूचना साझा की जाएगी।

5. संगठनात्मक सुरक्षा

क) एनसीवीईटी की जोखिम अनुपालन और डेटा सुरक्षा समिति एनसीवीईटी में सूचना जोखिम प्रबंधन और सूचना प्रौद्योगिकी सुरक्षा दोनों की निगरानी के लिए उत्तरदायी है। इसमें संगठन के समग्र कार्यनीतिक लक्ष्यों के भाग के रूप में सूचना परिसंपत्तियों के जोखिम और व्यक्तिगत सूचना प्रणालियों और संगठन की जोखिम सहनशीलता के अनुसार सुरक्षा के प्रबंधन जोखिम तथा कारोबारी सफलता सुनिश्चित करने के लिए अन्य प्रकार के जोखिम की निगरानी शामिल है।

ख) एनसीवीईटी के मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) सूचना सुरक्षा जोखिमों के मूल्यांकन और परामर्श के लिए उत्तरदायी होंगे।

ग) उपरोक्त बिंदुओं में उल्लिखित दोनों कार्य क्षेत्रों के साथ परामर्श करके सूचना सुरक्षा जोखिम निर्णय लिए जाएंगे।

घ) यद्यपि तकनीकी सूचना सुरक्षा कार्य आउटसोर्स या अनुबंधित किए जा सकते हैं, लेकिन एनसीवीईटी अपनी संबंधित सूचना की सुरक्षा के लिए समग्र जिम्मेदारी रखता है।

ड.) कार्यालय परिसर के भीतर और बाहर पीसी/ हार्डवेयर का स्थानांतरण करने के लिए मानक प्रक्रिया (एसओपी)

i. अप्रचालित सॉफ्टवेयर अपग्रेड किए जाएं,

ii. जिन पीसी हार्डवेयर की कार्य अवधि का समापन (ईओएल) हो गया है, उन्हें अप्रचालित घोषित किया जाए।

iii. पीसी/ डेस्कटॉप को दैनिक आधार पर बंद (शट डाउन) किया जाए।

iv. परामर्शदाताओं की एनसीवीईटी टीम की ऑनबोर्डिंग और ऑफबोर्डिंग के लिए मानक प्रक्रिया, जिससे उचित ऑनबोर्डिंग और उचित ऑफ बोर्डिंग की व्यवस्था होने से साइबर सुरक्षा बचाव में कमियों से बचा जा सकता है क्योंकि प्रस्थान करने वाले कर्मचारियों तक पहुंच हो सकती है।

6. कार्यात्मक जिम्मेदारियां

6.1. जोखिम अनुपालना और डेटा सुरक्षा समिति

समिति की अध्यक्षता डेटा, जोखिम, अनुपालना और प्रौद्योगिकी में विशेषज्ञ एनसीवीईटी के एक कार्यकारी सदस्य/निदेशक/नामित अधिकारी द्वारा की जाएगी। इस क्षेत्र के जानकार राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) का एक अधिकारी इस समिति का सदस्य हो सकता है। मुख्य सूचना सुरक्षा अधिकारी (सीओईएसओ) इस समिति का भाग होगा। समिति निम्नलिखित के लिए उत्तरदायी होगी :

i. एनसीवीईटी की ओर से जोखिम मूल्यांकन और स्वीकरण,

ii. सूचना सुरक्षा उत्तरदायित्वों और लक्ष्यों को पहचानना और उन्हें संगत प्रक्रियों में एकीकृत;

iii. सूचना सुरक्षा नीतियों और मानकों के सतत कार्यान्वयन में सहायता करना;

iv. उपयुक्त संसाधनों के स्पष्ट निर्देशन और प्रदर्शित प्रतिबद्धता के माध्यम से सुरक्षा सहायता;

v. सीआईएसओ द्वारा प्रदान की गई सामग्रियों के नियमित प्रसार के माध्यम से सूचना सुरक्षा श्रेष्ठ पद्धतियों की जानकारी को बढ़ावा देना;

vi. सूचना के संरक्षण के उपयुक्त स्तरों के निर्धारण के लिए उद्योग संस्तुत पद्धतियों, संगठन निर्देशों और कानूनी व नियामक अपेक्षाओं के आधार पर सूचना वर्गीकरण और श्रेणीकरण के निर्धारण की प्रक्रिया का कार्यान्वयन;

vii. सूचना वर्गीकरण और श्रेणीकरण के आधार पर सूचना परिसंपत्तियों की पहचान, संचालन, उपयोग, पारेषण और निपटान के लिए प्रक्रिया का कार्यान्वयन;

viii. यह निर्धारण करना कि किसे डेटा की गोपनीयता, प्रामाणिकता और उपलब्धता के लिए अंतिम जिम्मेदारी का रखरखाव करते समय सूचना स्वामियों के रूप में दायित्व और सेवा किसे सौंपी जाएगी।

ix. सुरक्षा घटनाओं की प्रतिक्रिया में भागीदारी

x. निजी सूचना का उल्लंघन होने की स्थित में अधिसूचना की अपेक्षाओं का पालन करना,

xi. सूचना सुरक्षा के संबंध में विशिष्ट कानूनी और नियामक अपेक्षाओं का पालन करना,

xii. सीआईएसओ को कानूनी और नियामक अपेक्षाओं की जानकारी देना; और इस नीति और संबद्ध मानकों की अनुपालना न किए जाने के परिणामों सहित उनकी अपेक्षाओं के बारे में कर्मचारियों और अन्य पक्षकारों में अनुपालना का समाधान करना;

xiii. स्वैच्छिक मूल्यांकन/नई संवेदनशीलताओं का पता लगाने के आधार पर नियमित सुरक्षा पैच अपडेट की समीक्षा करना।

6.2. मुख्य सूचना सुरक्षा अधिकारी

नियुक्त मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) निम्नलिखित के लिए उत्तरदायी होगा :

i. कारोबारी कार्यों और अपेक्षाओं जानकारी को समझना और रखरखाव करना;

ii. सूचना सुरक्षा से प्रत्यक्ष रूप से संबद्ध वार्षिक सतत व्यावसायिक शिक्षा (सीपीई) क्रेडिट के माध्यम से सूचना सुरक्षा में वर्तमान ज्ञान प्रवीणता का पर्याप्त स्तर सुनिश्चित करना;

iii. सूचना सुरक्षा नीतियों और कानूनी व नियामक सूचना सुरक्षा अपेक्षाओं की अनुपालना का मूल्यांकन करना;

iv. सूचना सुरक्षा जोखिमों का मूल्यांकन करना और समझना तथा उन जोखिमों का उपयुक्त प्रबंधन करना;

v. यह दर्शाना और आश्वस्त करना कि सुरक्षा वास्तुकीय चिंताओं का समाधान किया गया है।

vi. उत्पादों और सेवाओं की खरीद के संबंध में सुरक्षा संबंधी चिंताओं पर परामर्श देना।

vii. बढ़ती सुरक्षा चिंताएं, जिनका लागू सूचना और विस्तार प्रक्रियाओं के अनुसार पर्याप्त समाधान नहीं किया गया है;

viii. उपयुक्त पक्षों को खतरे की सूचना प्रसारित करना;

ix. संभावित सुरक्षा घटनाओं के प्रत्युत्तर में भागीदारी करना,

x. ऐसी उद्यम नीतियों और मानकों के विकास में भागीदारी करना, जिन्हें संगठन की जरूरत माना गया है;

xi. सूचना सुरक्षा जागरूकता को बढ़ावा देना;

xii. अपेक्षानुसार सुरक्षा परामर्शदाताओं के रूप में आंतरिक विशेषज्ञ प्रदान करना;

xiii. प्रभावकारिता के उपायों सहित सुरक्षा कार्यक्रम और रणनीति का विकास करना;

xiv. उद्यम सूचना सुरक्षा नीति और मानकों की स्थापना और रखरखाव करना;

xv. सुरक्षा नीतियों और मानकों के अनुपालन का मूल्यांकन करना;

xvi. सुरक्षित प्रणाली इंजीनियरी पर परामर्श देना;

xvii. घटना प्रतिक्रिया समन्वयन और विशेषज्ञता प्रदान करना;

xviii. डेटा उल्लंघनों छेड़छाड़ आदि के संकेतों के लिए विसंगतियों और बाहरी स्रोतों के लिए निगरानी नेटवर्क;

xix. सुरक्षा समूहों/ एसोसिएशनों और संगत प्राधिकारियों के साथ वर्तमान संपर्क को बनाए रखना;

xx. वर्तमान खतरों और संवेदनशीलताओं की समय पर अधिसूचना प्रदान करना;

xxi. जागरूकता सामग्री और प्रशिक्षण संसाधन प्रदान करना;

xxii. नियमित सुरक्षा जांच सुनिश्चित करना;

xxiii. आईएसओ 27001 की अनुपालना सुनिश्चित करना और आईएसओ 27002 प्रक्रियाओं का अंगीकरण करना;

xxiv. भारत सरकार की डेटा निजता नीति के अनुसार एनसीवीईटी के विभिन्न हितधारकों के लिए रखी गई सूचना के लिए अपेक्षानुसार डेटा एंक्रिप्शन लागू करना;

xxv. सूचना के स्वामियों की सहायता करने वाले डेटा प्रोसेसिंग इंफ्रास्ट्रक्चर और कंप्यूटरिंग नेटवर्क में सुरक्षा नियंत्रणों का स्पष्ट निर्देशन प्रदान करना और विचार करना;

xxvi. संगठनात्मक नीति के अनुसार सूचना सुरक्षा नियंत्रण का स्तर बनाए रखने के लिए अपेक्षित संसाधनों की आपूर्ति करना;

xxvii. कारोबारी द्वारा परिभाषित सुरक्षा अपेक्षाओं के संबंध में सभी प्रक्रियाओं, नीतियों और नियंत्रणों की पहचान और कार्यान्वयन करना;

xxviii. वर्गीकरण के आधार पर स्वामित्व वाली सूचना के लिए उचित नियंत्रण लागू करना;

xxix. सुरक्षित प्रचालनों (अर्थात सुरक्षित कोटिंग, सुरक्षित कांफिगुरेशन) के संबंध में उपयुक्त तकनीकी स्टॉफ को प्रशिक्षण प्रदान करना।

xxx. सूचना परिसंपत्तियों का संरक्षण करने में और उपयुक्त व किफायती सुरक्षा नियंत्रण और प्रक्रियाओं की पहचान, चयन और कार्यान्वयन में सूचना सुरक्षा और तकनीकी स्टॉफ की भागीदारी बढ़ाना;

xxxi. क्षतिग्रस्त प्रणालियों से कारोबारी निरंतरता और आपदा बहाली योजनाओं का कार्यान्वयन करना;

xxxii. अज्ञात/ संदिग्ध पहुंच/ सूचना/ खतरे सहित प्रणाली की पहुंच के संबंध में डेशबोर्ड प्रदान करना।

6.3. कर्मचारी, परामर्शदाता और अन्य पक्ष

ऐसे कर्मचारी, परामर्शदाता, उप परामर्शदाता और अन्य पक्ष, जो एनसीवीईटी को अपनी सेवाएं प्रदान कर रहे हैं, निम्नलिखित के लिए उत्तरदायी होंगे :

i. प्रदान की गई सूचना की गोपनीयता, प्रामाणिकता और उपलब्धता को संरक्षित रखने के लिए बेसलाइन सूचना सुरक्षा नियंत्रणों को समझना;

ii. सूचना और संसाधनों का अनधिकृत उपयोग और प्रकटन से संरक्षण प्रदान करना;

iii. व्यक्तिगत, निजी, संवेदनशील सूचना का अनधिकृत उपयोग और प्रकटन होने से संरक्षण प्रदान करना;

iv. सूचना प्रौद्योगिकी संसाधन नीति के स्वीकार्य उपयोग का पालन करना;

v. उपयुक्त प्रबंधन और सीआईएसओ/ निर्दिष्ट सुरक्षा प्रतिनिधि को संदिग्ध सूचना सुरक्षा घटनाओं अथवा कमजोरियों की सूचना देना।

7. कर्त्तव्यों का पृथक्करण

क) दुर्घटनात्मक अथवा सुविचारित प्रणाली के दुरुपयोग के जोखिम को कम करने के लिए, एनसीवीईटी, जहां कहीं उपयुक्त है, कर्त्तव्यों के पृथक्करण और जिम्मेदारी के क्षेत्रों को स्पष्ट रूप से निर्दिष्ट करेगी।

ख) जब भी कर्त्तव्यों का पृथक्करण तकनीकी रूप से व्यवहार्य नहीं हो, अन्य प्रतिपूरक नियंत्रणों को कार्यान्वित किया जाएगा जैसे क्रियाकलापों की निगरानी, ऑडिट ट्रेल और प्रबंधन पर्यवेक्षण।

ग) सुरक्षा नियंत्रणों का ऑडिट और अनुमोदन प्रायः स्वतंत्र रहेगा और सुरक्षा नियंत्रणों के कार्यान्वयन से पृथक होगा।

8. प्रमुख क्षेत्रों पर नीति की प्रयोज्यता

8.1. नेटवर्किंग और अवसंरचना सुरक्षा

इसमें सर्वर, प्लेटफार्म, नेटवर्क, संचार डेटावेस और सॉफ्टवेयर अनुप्रयोग शामिल है, लेकिन यह केवल इन्हीं तक सीमित नहीं है *("राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) की इसके सूचना और संचार प्रौद्योगिकी (आईसीटी) नेटवर्क - निकनेट के माध्यम से" सुरक्षा नीति के संदर्भ में)*

i. एनसीवीईटी के सीआईएसओ अथवा उसके द्वारा नियुक्त एक निर्दिष्ट व्यक्ति/ समूह एनसीवीईटी की ओर से नियुक्त किसी प्रणाली के रखरखाव और प्रशासन के लिए जिम्मेदारी ग्रहण करेगा। उत्तरदायी व्यक्तियों अथवा समूहों की एक सूची केंद्रीय रूप से रखी जाएगी।

ii. प्रणाली की शुरुआत में सुरक्षा पर विचार किया जाएगा और एक प्रणाली के सृजन अथवा संशोधन के लिए निर्णय के भाग के रूप में दस्तावेजीकरण किया जाएगा।

iii. प्रत्येक प्रणाली में किसी ऐसे डेटा के वर्गीकरण के अनुसार अनेक नियंत्रण स्थापित किए जाएंगे, जिन्हें स्टोर किया गया और अनुमत किया गया।

iv. सभी सिस्टम घड़ियां एनटीसी (यूनिवर्सल टाइम) पर सेट एक केंद्रीकृत संदर्भ समय के साथ समकालिक (सिंक्रनाइज) की जाएंगी, जो अपने आप ही कम से कम तीन समकालिक समय स्रोतों के साथ समकालिक की गई है।

8.2. डेटाबेस और सॉफ्टेवयर (आंतरिक अथवा अन्य पक्ष द्वारा विकसित और पहले से तैयार वाणिज्यिक सहित (सीओटीएस)

(निकनेट सुरक्षा नीति के संदर्भ में)

क) एनसीवीईटी अथवा इसेक संगत पक्षों के संबंध में एससीवीईटी को संवेदनशील सूचना अथवा डेटा तक पहुंच वीपीएन जैसे सुरक्षित कनेक्शनों के माध्यम से दी जाएगी।

ख) सिस्टम के लिए अथवा सिस्टम पर परिनियोजित किए गए सभी सॉफ्टवेयर में सुरक्षित कोडिंग पद्धतियां शामिल होनी चाहिए ताकि सामान्य कोडिंग संवेदनशीलताओं की घटना से बचा जा सके और उत्पादन में शामिल किए जाने से पूर्व अत्यधिक जोखिम वाले खतरों को लचीला बनाया जाए।

ग) एक बार डेटा की तैनाती किए जाने के बाद, डेटा के वर्गीकरण के अनुसार परीक्षण समय के लिए उसे संरक्षित और नियंत्रित किया जाना चाहिए।

घ) उत्पादन डेटा का उपयोग केवल परीक्षण के लिए किया जाए, यदि एक कारोबारी मामले का सूचना स्वामी द्वारा लिखित में दस्तावेज किया जाता है और अनुमोदित काय जाता है और निम्नलिखित नियंत्रण लागू किया जाता है :

- उत्पादन डेटा के लिए सभी सुरक्षा उपाय, जिसमें पहुंच नियंत्रण, प्रणाली कांफिगुरेशन और लॉगिंग अपेक्षाएं शामिल हैं लेकिन इन्ही तक सीमित नहीं है, परीक्षण वातावरण में लागू के जाते हैं और परीक्षण पूरा होते ही डेटा को डिलीट किया जाता है।
- संवेदनशील डेटा काल्पनिक सूचना से ढक दिया जाता है या ऊपर अधिलेखित कर दिया जाता है।

ड.) जहां तकनीकी रूप से व्यवहार्य हो, विकास सॉफ्टवेयर और उपकरणों का उत्पादन प्रणालियों पर रखरखाव नहीं किया जाना चाहिए।

च) जहां तकनीकी रूप से व्यवहार्य हो, एक एप्लिकेशन अथवा सॉफ्टेवयर तैयार करने के लिए प्रयुक्त स्रोत कोड को उस एप्लिकेशन अथवा सॉफ्टवेयर के चलाने वाली उत्पादन प्रणाली पर स्टोर नहीं करना चाहिए।

छ) उत्पादन प्रणालियों से स्क्रिप्ट को हटा दिया जाए, केवल ऐसे मामलों को छोड़कर, जहां सिस्टम के प्रचालन और रखरखाव के लिए उनकी आवश्यकता हो।

ज) विकसित करने वाले स्टॉफ द्वारा उत्पादन प्रणालियों तक विशेष पहुंच को सीमित किया जाए।

झ) माइग्रेशन प्रक्रियाओं का दस्तावेजीकरण किया जाए और उत्पादन परिवेश के माध्यम से विकास परिवेश से सॉफ्टवेयर को स्थानांतरण के संचालन के लिए उसे कार्यान्वित किया जाए।

ञ) परिवेशों को पृथक्करण (अर्थात विकास, परीक्षण, गुणवत्ता आश्वासन उत्पादन) की पृथक परिवेशीय सहित तर्कसंगत रूप से अथवा भौतिक रूप से व्यवस्था की जाए।

ट) वैधीकरण परिवेशों और परीक्षण योजनाओं को तैयार किया जाना चाहिए ताकि उत्पादन में तैनाती से पूर्व सिस्टम सही ढंग से कार्य करे।

ठ) सभी सिस्टम के लिए औपचारिक परिवर्तन नियंत्रण कार्यविधियां, जिसमें कोई बदलाव शामिल है, जो उत्पादन परिवेश या डेटा पर संभावित प्रभाव डाल रही है, विकसित की जाएं और एनसीवीईटी की किसी प्रणाली के लिए लागू की जाए।

8.3. नेटवर्क सिस्टम

(निकनेट सुरक्षा नीति के संदर्भ में)

(क) प्रणालियों के बीच कनेक्शन को सभी संगत संस्थाओं के एनसीवीईटी के सीआईएसओ द्वारा अधिकृत किया जाए और उपयुक्त नियंत्रणों के कार्यान्वयन द्वारा संरक्षित किया जाए।

(ख) सभी कनेक्शन और उनके कांफिगुरेशन का दस्तावेजीकरण किया जाए और दस्तावेजों की सूचना स्वामी और सीआईएसओ/ निर्दिष्ट सुरक्षा प्रतिनिधि द्वारा कम से कम वार्षिक रूप से सीमीक्षा की जाए, ताकि यह सुनिश्चित हो सके कि:

- कनेक्शन के लिए कारोबारी मामला अभी वैध है और कनेक्शन अभी चाहिए; और
- लागू सुरक्षा नियंत्रण (फिल्टर नियम, पहुंच नियंत्रण सूची आदि) उपयुक्त है और सही तरीके से कार्य कर रहा है।

(ग) एक नेटवर्क आर्किटेक्चर का रखरखाव किया जाए जिसमें निम्नलिखित के बीच एक न्यूनतम, स्तरीय नेटवर्क सेगमेंटेशन शामिल है :

- इंटरनेट सुगम प्रणालियां और आन्तरिक प्रणालियां
- उच्च सुरक्षा श्रेणीकरण (अर्थात मिशन क्रिटिकल, पीआईआई वाली प्रणालियां) और अन्य प्रणालियों वाली प्रणालियां; और
- यूजर और सर्वर सेगमेंट।

घ) नेटवर्क प्रबंधन को एक सुरक्षित, समर्पित नेटवर्क से किया जाए।

ड.) इंटरनेट प्रणालियों से जुड़ने वाले साबी यूजर के लिए प्रमाणीकरण आवश्यक है।

च) इंटरनेट प्रणालियों से जुड़ने वाले सभी उपकरणों के लिए नेटवर्क प्रमाणीकरण आवश्यक है।

छ) केवल अनधिकृत व्यक्ति या कारोबारी इकाइयां है नेटवर्क ट्रेफिक को प्राप्त अथवा मॉनीटर कर सके।

ज) सीआईएसओ/ निर्दिष्ट सुरक्षा प्रतिनिधि के परामर्श से किसी भी नेटवर्क टेक्नोलॉजी या परियोजना में, जिसमें वायरलेस टेक्नोलॉजी शामिल है लेकिन केवल इस तक सीमित नहीं है, शुरू करने अथवा महत्वपूर्ण परिवर्तन करने से पूर्व एक जोखिम मूल्यांकन किया जाए।

झ) जोखिम विश्लेषण में, सहायता वाले अज्ञात आईपी/ स्थानों से उपयोग सहित नेटवर्क/ संसाधन उपयोग डेशबोर्ड प्रदान किया जाए।

8.4. पहचान, पहुंच और विशेषाधिकार प्रबंधन

क. ऑफलाइन आईटी अवसंरचना :

i. उपकरणों की सुरक्षा विशेषताओं के आधार पर जैसे एक्सेस नियंत्रण, ऑडिट और जबावदेही, पहचान और प्रमाणीकरण, उपकरणों की निम्नलिखित सूची को एमसीडीई लेपटॉप के निकनेट में प्रचालनों की अनुमति हैः

1. मोबाइल
2. टेबलेट
3. नेटवर्क प्रिंटर
4. वीसी सिस्टम
5. स्मार्ट टीवी
6. बाहरी स्टोरेज उपकरण जैसे पेन ड्राइव, केवल पहचाने गए बाहरी स्टोरेज उपकरणों की अनुमति होगी।
7. प्रत्येक पीसी/ ऐंड प्वाइंट के लिए एनआईसी द्वारा संस्तुत अनिवार्य वीईएम/ ईडीआर एजेंट कांफिगुरेशन
8. नेटवर्क सर्वर कक्ष में प्रवेश के लिए सीमित पहुंच

ii. डेस्कटॉप के मामले में, एडमिनिस्ट्रेटिव और यूजर एक्सेस सेपरेशन अनिवार्य है। यदि यूजर को प्रशासन के अधिकार प्रदान किए जाते हैं, तो

वे इंटरनेट पर उपलब्ध कोई सॉफ्टवेयर लगा सकते हैं और इसलिए सिस्टम और नेटवर्क को खतरे में डाल सकते हैं। अधिकारियों के दैनिक प्रचालनों के लिए प्रत्येक डेस्कटॉप पर एक सामान्य यूज़र बनाया जाना चाहिए। एमएसी बाध्यता डेस्कटॉप और स्मार्ट टीवी के लिए अनिवार्य है।

iii. अनधिकृत एक्सेस, भौतिक क्षति और आईटी प्रणाली में टेम्परिंग को भौतिक सुरक्षा लागू करके मॉनीटर किया जाए। महत्वपूर्ण/ संवेदनशील जोन की मॉनिटरिंग सीसीटीवी कैमरे के माध्यम से की जाए और फुटेज को कम से कम 180 दिनों के लिए स्टोर की जाए।

iv. संगठन यह सुनिश्चित करे कि नेटवर्क उपकरण और सूचना प्रणालियों के डिफाल्ट क्रेडेंशियल जैसे यूजरनेम, पासवर्ड और टोकन को उन्हें लगाए जाने अथवा प्रथम उपयोग किए जाने से पहले बदला जाए। यूजर के स्तर पर सभी उपकरण यूजर अकाउंट का प्रयोग करें और प्रशासक के अकाउंट का उपयोग केवल नेटवर्क/ सिस्टम प्रशासकों के लिए सीमित होना चाहिए।

ख. ऑनलाइन आईटी अवसंरचनाः

i. केवल सरकारी ईमेल आईडी का प्रयोग सरकारी कार्य के लिए किया जाए।

ii. सरकारी प्रणाली पर बनाए जा रहे सभी अकाउंट और एनसीवीईटी की प्रमुख आईटी टीम/ सीआईएसओ की अगुवाई में थर्ड पार्टी वेंडर द्वारा प्रबंधित अकाउंट।

iii. अकाउंट प्रबंधन/ एक्सेस नियंत्रण मानक में यथा निर्दिष्ट को छोड़कर व्यक्तिगत रूप से प्रदत्त यूनीक आइडेंटीफायर, जिसे यूजर आईडी के नाम से जाना जाता है, का उपयोग करके सिस्टम में एक्सेस प्रदान की जाएगी।

iv. प्रत्येक यूजर आईडी के साथ, एक प्रमाणीकरण टोकन (अर्थात, पासवर्ड की-फोब, बायोमेट्रिक) का प्रयोग एक्सेस का अनुरोध करने वाले व्यक्ति या सिस्टम की पहचान को प्रमाणित करने के लिए किया जाए। पासवर्ड में निम्नलिखित मानकों को पूरा किया जाएः

क) कम से कम 8 अक्षर का हो,

ख) कम से कम एक अपर केस और एक लोवर केस अक्षर होना चाहिए।

ग) कम से कम एक विशेष वर्ण (स्पेशल करेक्टर) होना चाहिए।

घ) अक्षरांकीय (अल्फा न्यूमेरिक) होना चाहिए।

v. पासवर्ड को हर 6 माह में बदला जाए और मोबाइल नम्बर के साथ लिंक होना चाहिए। एक सेसन को लॉक करने के लिए ऑटोमेटेड तकनीक और नियंत्रण होना चाहिए और जहां प्रमाणीकरण आवश्यक हो, किसी सिस्टम के लिए निष्क्रिय रहने की अवधि के कम प्रमाणीकरण और पुनः प्रमाणीकरण आवश्यक होना चाहिए। कंपनी के संबंध में डेटा प्राप्त करते समय, यूजर यह सुनिश्चित करें कि स्क्रीन पर सूचना को सेसन लॉक के दौरान सार्वजनिक कम रूप से देखी जाने वाली सूचना (अर्थात स्क्रीन सेवर, ब्लैंक स्क्रीन, क्लॉक) से बदला जाए। निष्क्रियता के मामले में, अथवा जब ये उपकरण प्रयोग में लाए जाते हैं, यूजर यह सुनिश्चित करे कि इन उपकरणों को अच्छी तरह से लॉक किया गया है।

vi. किसी व्यक्ति या प्रक्रिया के प्रमाणीकरण के लिए प्रयुक्त टोकन को गोपनीय माना जाए और उपयुक्त रूप से संरक्षित किया जाए।

vii. सूचना स्वामी यह निर्धारण करने के लिए उत्तरदायी हैं कि किसे उनके क्षेत्राधिकार में संरक्षित संसाधनों तक पहुंच (एक्सेस) होनी चाहिए और वह विशेषाधिकार एक्सेस क्या होगा (पठन, अपडेट आदि)

viii. यूजर की जॉब उत्तरदायित्वों के अनुसार एक्सेस का विशेषाधिकार प्रदान किया जाएगा और वह एनसीवीईटी मिशनों और कारोबारी कार्यों के अनुसार प्रदान किए गए कार्यों को पूरा करने के लिए आवश्यकता तक ही सीमित होगा (अर्थात न्यूनतम विशेषाधिकार) ।

ix. विशेषाधिकार वाले अकाउंट के यूजर सामान्य कारोबार करते समय एक अलग, गैर विशेषाधिकार वाले अकाउंट का प्रयोग करें।

x. किसी रिमोट एक्सेस कनेक्शन के लिए एनसीवीईटी द्वारा अग्रिम अनुमोदन प्रदान किया जाए। एक्सेस के कार्यक्षेत्र और विधि में शामिल तकनीकी और कारोबारी जोखिम और अनुबंध, प्रक्रिया और तकनीकी नियंत्रण के निर्धारण के लिए, जो ऐसे कनेक्शन के लिए अपेक्षित है, एक मूल्यांकन किया जाए और दस्तावेजीकरण किया जाए।

xi. सभी रिमोट कनेक्शन प्रबंधित प्रवेश बिन्दु के माध्यम से किए जाए, जिनकी सीआईएसओ/ निर्दिष्ट सुरक्षा प्रतिनिधि द्वारा समीक्षा की जाए।

xii. रिमोट स्थान से कार्य को प्रबंधन द्वारा अधिकृत किया जाए और रिमोट परिवेश में डेटा का उपयुक्त संरक्षण सुनिश्चित करने के लिए पद्धतियों को रिमोट एक्सेस प्रदान किए जाने वाले व्यक्ति से पहले व्यक्तियों के साथ साझा किया जाए।

8.5. सुरक्षित क्लाउड सेवाएं *(निकनेट सुरक्षा नीति के संदर्भ में)*

i. क्लाउड सेवाओं में सुरक्षा और अनुपालन के लिए साझा किए गए जिम्मेदारी मॉडल की पूरी तरह से जांच करें।

ii. क्लाउड सेवाओं पर डाले गए परीक्षण, स्टेजिंग और बैकअप परिवेशों के लिए उपयुक्त सुरक्षा नीतियों और उपायों को कार्यान्वित करें।

iii. प्रयोग में आने वाले सभी क्लाउड दृष्टांत की सार्वजनिक पहुंच को सत्यापित करें।

iv. यह सुनिश्चित करें कि कोई सर्वर, स्टोरेज अनुपयुक्त कांफिगुरेशन के कारण गलती से भी कोई डेटा लीक तो नहीं कर रहा है।

v. क्लाउड संसाधनों की ग्रेन्युलर अनुमति के साथ एक्सेस नियंत्रण के लिए न्यूनतम विशेषाधिकार सिद्धांत लागू करें।

vi. महत्वपूर्ण क्लाउड संसाधनों के लिए क्लाउड नेटिव सुरक्षा नियंत्रण और लॉगिंग सक्षम करें।

vii. अधिक सुरक्षा के साथ इन संसाधनों की निरंतर निगरानी सुनिश्चित करें।

viii. यह सुनिश्चित करें कि यूजर अकाउंट में मल्टी फेक्टर प्रमाणीकरण (एमएफए) के साथ-साथ एक सख्त पासवर्ड नीति हो।

ix. जब कोई प्रशासक/ यूजर किसी संगठन को छोड़ता है, तो अकाउंट को अक्षम (डिसेबल) करने के लिए एक प्रक्रिया/ मानक लागू करें।

8.6. भौतिक और पर्यावरणीय सुरक्षा

i. सूचना प्रसंस्करण और भंडारण सुविधाओं के लिए एक परिभाषित सुरक्षा व्यवस्था और उपयुक्त सुरक्षा अवरोध और एक्सेस नियंत्रण होना चाहिए।

ii. सूचना प्रसंस्करण और भंडारण सुविधाओं के लिए एक आवधिक जोखिम मूल्यांकन किया जाना चाहिए ताकि यह निर्धारण किया जा सके कि क्या मौजूदा नियंत्रण सही तरीके से किए जा रहे हैं और क्या अतिरिक्त भौतिक सुरक्षा उपाय आवश्यक हैं। इन उपायों को जोखिमों में कमी लाने के लिए कार्यान्वित किया जाए।

iii. सूचना प्रौद्योगिकी उपकरणों को सुरक्षा आशंकाओं और पर्यावरणीय खतरों से भौतिक रूप से संरक्षित किया जाए। सहायक अवसंरचना और सुविधाओं जैसे विद्युत आपूर्ति और केबल अवसंरचना के संरक्षण के लिए विशेष नियंत्रण भी आवश्यक हो सकते हैं।

iv. समस्त सूचना प्रौद्योगिकी उपकरण और सूचना मीडिया को उनमें निहित सूचना के वर्गीकरण के अनुसार गोपनीयता, प्रामाणिकता, अथवा उपलब्धता से समझौता होने को संरक्षण देने के लिए सुरक्षित किया जाना चाहिए।

v. सूचना प्रसंस्करण और भंडारण सुविधाओं के रखरखाव कार्मिकों सहित आगंतुकों की हर समय सहायता की जाए।

8.7. डेटा सुरक्षा और संचालन

i. ऐसी प्रणाली या प्रक्रिया, जो कारोबार डेटा में सहायता करती है, एक सुरक्षित प्रणाली विकास समय अवधि के भाग के रूप में कम से कम वार्षिक रूप से सूचना जोखिम और सूचना जोखिम मूल्यांकन के लिए उपयुक्त रूप से प्रबंधित की जाए।

ii. नई परियोजनाओं, नई प्रौद्योगिकियों के कार्यान्वयन, प्रचालन परिवेश में महत्वपूर्ण परिवर्तनों या किसी महत्वपूर्ण संवेदनशीलता को प्रकट करने के परिणामस्वरूप सूचना सुरक्षा जोखिम का मूल्यांकन आवश्यक है।

iii. जोखिम मूल्यांकन परिणाम और इन परिणामों के आधार पर लिए गए निर्णयों का दस्तावेजीकरण किया जाए।

iv. समस्त सूचना, जो व्यावसायिक क्रियाकलापों के समर्थन में तैयार, अर्जित या उपयोग की गई है, उसका उपयोग केवल उसके इच्छित व्यावसायिक उद्देश्य के लिए ही किया जाए।

v. समस्त सूचना प्रौद्योगिकियों के लिए व्यावसाय की सीमा के भीतर एक सूचना स्वामी होना चाहिए। उन्हें डेटा गोपनीयता दिशानिर्देशों पर भी प्रशिक्षित किया जाए।

vi. सूचना को तैयार करने से लेकर उसके अधिकृत उपयोग और निपटान किए जाने तक सावधानीपूर्वक प्रबंधित किया जाए। प्रत्येक परिसंपत्तियों को उसके निजी डेटा तत्वों द्वारा आवश्यक उच्चतम स्तर पर वर्गीकृत किया जाए।

vii. यदि एनसीवीईटी सूचना के गोपनीय वर्गीकरण को निर्धारित करने में असमर्थ है, अथवा सूचना निजी पहचान सूचना (पीआईआई) है, तो सूचना का गोपनीय वर्गीकरण होना चाहिए और इसलिए यह गोपनीयता नियंत्रण के अंतर्गत है।

viii. सूचना का विलय होने से एक नई सूचना परिसंपत्ति निर्मित होती है या ऐसी परिस्थितियां, जो विलय की संभावना उत्पन्न करती हैं, (उदाहरण के लिए अनेक फाइलों के साथ बैकअप टेप) उनका यह निर्धारित करने के लिए मूल्यांकन किया जाए कि विलय किए गए डेटा का नया वर्गीकरण करने की आवश्यकता है अथवा नहीं।

ix. सूचना की समग्रता में सभी प्रतिकृतियों में मूल के समान ही गोपनीयता वर्गीकरण किया जाए। यह निर्धारित करने के लिए कि क्या नया वर्गीकरण आवश्यक है, आंशिक प्रतिकृतियों का मूल्यांकन किया जाए।

x. प्रत्येक वर्गीकरण में इन वर्गीकरणों की सुरक्षा के लिए किए गए मूलभूत नियंत्रणों का एक स्वीकृत सेट होता है, और इन नियंत्रणों की अनुपालना की जाए।

xi. एनसीवीईटी को अपने कर्मचारियों को सूचना के सुरक्षित संचालन की आवश्यकता के संबंध में बताया जाना चाहिए।

xii. सभी सूचना परिसंपत्तियों की एक लिखित या इलैक्टॉनिक सूची रखी जाए।

xiii. आम जनता के लिए उपलब्ध कराई गई सामग्री की समीक्षा, एक ऐसी प्रक्रिया के अनुसार की जाए, जिसे एनसीवीईटी द्वारा परिभाषित और अनुमोदित किया जाएगा। इस प्रक्रिया में सार्वजनिक रूप से उपलब्ध सामग्री के अपडेट की समीक्षा और अनुमोदन शामिल होना चाहिए और उपलब्ध कराई गई सूचना के प्रकार और वर्गीकरण पर विचार किया जाए।

xiv. एनसीवीईटी द्वारा अनुमोदित उचित सुरक्षा उपायों के बिना निजी पहचान योग्य सूचना (पीआईआई) उपलब्ध नहीं कराई जाए।

xv. एनसीवीईटी से बाहर जारी की जाने वाली या अन्य संस्थाओं के बीच साझा की जाने वाली गैर-सार्वजनिक सूचना के लिए एक प्रक्रिया स्थापित की जाए, जो कम से कम :

   क. जारी की जाने वाली या साझा की जाने वाली सूचना की संवेदनशीलता का मूल्यांकन और दस्तावजीकरण करें;

   ख. सूचना की सुरक्षा के लिए प्रत्येक पक्ष की जिम्मेदारी की पहचान करें;

   ग. सूचना को प्रेषित करने और उपयोग करने के लिए आवश्यक न्यूनतम नियंत्रणों को परिभाषित करें;

   घ. सूचना की सुरक्षा के लिए प्रत्येक पक्ष द्वारा अपनाए गए उपायों को रिकार्ड करें;

   ड. अनुपालन के मापन के लिए एक तरीका निर्दिष्ट करें;

च. प्रत्येक पक्ष के लिए उत्तरदायित्वों को स्वीकार करने के लिए एक साइन ऑफ प्रक्रिया प्रदान करें;

छ. नियंत्रणों की समीक्षा के लिए एक कार्यक्रम और प्रक्रिया स्थापित करें।

8.8. खतरा और संवेदनशीलता प्रबंधन

i. सभी प्रणालियों को उत्पादन में स्थापित किए जाने से पूर्व और उसके बाद समय-समय पर उनकी सुभेद्यता के लिए स्केन किया जाए।

ii. सभी प्रणालियां आवधिक प्रवेश परीक्षण के अध्यधीन हैं।

iii. सभी महत्वपूर्ण परिवेशों/ प्रणालियों के लिए समय-समय पर प्रवेश परीक्षण की आवश्यकता होती है।

iv. जहां एनसीवीईटी ने किसी अन्य इकाई या किसी अन्य पक्ष को सिस्टम आउटसोर्स किया है, वहां उनकी सुभेद्यता की स्कैनिंग/प्रवेश परीक्षण का समन्वयन किया जाए और उसका दस्तावेजीकरण किया जाए।

v. स्कैनिंग/ परीक्षण और उपशमन को अन्य पक्ष समझौतों में शामिल किया जाए।

vi. स्केन/ प्रवेश परीक्षण के आउटपुट की सीआईएसओ द्वारा समय-समय पर समीक्षा की जाए। जोखिम के मूल्यांकन के लिए स्केन रिपोर्ट/ प्रवेश परीक्षा की प्रतियां सीआईएसओ/ नामित सुरक्षा प्रतिनिधि के साथ साझा की जाए।

vii. प्रकट की गई सुभेद्यताओं का समाधान करने के लिए सिस्टम को पैच करने या अपडेट करने जैसी उचित कार्रवाई की जाए। किसी भी प्रकार की सुभेद्यता के लिए एक कार्य योजना और लक्ष्य तय किया जाए और सुभेद्यता को कम करने के लिए नियोजित उपचारी कार्रवाई का दस्तावेजीकरण करने के लिए तदनुसार अपडेट किया जाए।

viii. किसी भी सुभेद्यता की स्कैनिंग/ प्रवेश परीक्षण को ऐसे व्यक्तियों द्वारा संचालित किया जाए, जो सीआईएसओ/ नामित सुरक्षा प्रतिनिधि द्वारा अधिकृत हो। सीआईएसओ को ऐसे किसी भी परीक्षण के बारे में पहले से सूचित किया

जाए। इस तरह की सुभेद्यता स्कैनिंग/ प्रवेश परीक्षण किए जाने के किसी भी अन्य प्रयास को अनधिकृत पहुंच का प्रयास माना जाएगा।

ix. सुभेद्यता स्कैनिंग/ प्रवेश परीक्षण करने के लिए अधिकृत किसी भी व्यक्ति के पास व्यवधान की संभावना को कम करने के लिए हर समय एक औपचारिक प्रक्रिया निर्धारित की जाएं। परीक्षण किया जाए और उसका पालन किया जाए तथा उसे भारत सरकार के सीईआरटी-आईएन से मान्यताप्राप्त/ पैनलबद्ध होना चाहिए।

x. सभी सॉफ्टवेयरों के लिए पहुंच परीक्षण एसटीक्यूसीसी - मानकीकरण परीक्षण और गुणवत्ता प्रमाणन (एसटीक्यूसीसी), इलैक्ट्रोनिकी और सूचना प्रौद्योगिकी मंत्रालय से अधिकृत निकायों द्वारा किया जाए।

8.9. कार्मिक सुरक्षा

i. कर्मचारियों को उनकी नियुक्ति के 30 दिनों के भीतर सामान्य सुरक्षा जागरूकता प्रशिक्षण प्रदान किया जाए, जिसमें आन्तरिक खतरों की पहचान करना और रिपोर्ट करना शामिल है। यदि आवश्यक हो तो विशिष्ट सुरक्षा प्रक्रियाओं पर अतिरिक्त प्रशिक्षण, एनसीवीईटी संवेदनशील जानकारी तक पहुंच प्रदान करने से पूर्व पूरा किया जाए, जो सामान्य सुरक्षा प्रशिक्षण में शामिल नहीं है। सभी सुरक्षा प्रशिक्षण कम से कम वार्षिक रूप से सुदृढ़ किए जाएं और एनसीवीईटी द्वारा उन पर ट्रेक रखा जाए।

ii. एनसीवीईटी को अपने कर्मचारियों से सूचना प्रौद्योगिकी संसाधनों की नीति के स्वीकार्य उपयोग का पालन करने की आवश्यकता होनी चाहिए और उपभोक्ताओं के लिए एक ऑडिट करने योग्य प्रक्रिया होनी चाहिए ताकि वे स्वीकार कर सकें कि वे नीति की आवश्यकताओं का पालन करने के लिए सहमत हैं।

iii. सीआईएसओ द्वारा सभी जॉब पदों का मूल्यांकन किया जाना चाहिए ताकि यह निर्धारित किया जा सके कि उन्हें संवेदनशील सूचना और/ या संवेदनशील सूचना प्रौद्योगिकी परिसंपत्तियों तक पहुंच की आवश्यकता है अथवा नहीं।

iv. ऐसी जॉब पदों के लिए, जिनके लिए संवेदनशील सूचना और संवेदनशील सूचना प्रौद्योगिकी परिसंपत्तियों तक पहुंच आवश्यक है, एनसीवीईटी कर्मचारियों की उपयुक्तता का निर्धारण करेगी, जब तक कि कानून, नियमन या अनुबंध द्वारा ऐसा करने से प्रतिबंधित नहीं किया गया हो। जोखिम के स्तर के आधार पर, उपयुक्तता के निर्धारण में उचित और अनुमत के रूप में उसमें संघीय, राज्य और निजी स्रोतों से आपराधिक इतिहास रिकार्ड की सूचना या अन्य रिपोर्टों का मूल्यांकन शामिल हो सकता है, जो सार्वजनिक और गैर-सार्वजनिक रिकार्ड का रखरखाव करते हैं। उपयुक्तता निर्धारण में एनसीवीईटी को यह निष्कर्ष निकालने के लिए उचित आधार प्रदान करना चाहिए कि कोई व्यक्ति एनसीवीईटी के लिए अनुचित जोखिम के बिना संबंधित पद के अपेक्षित कर्त्तव्यों और उत्तरदायित्वों को निभाने में सक्षम होगा।

v. एनसीवीईटी में समय-समय पर और जॉब कर्त्तव्यों अथवा पद में परिवर्तन होने पर उपयुक्तता निर्धारण को दोहराने या समीक्षा करने के लिए एक प्रक्रिया स्थापित की जाएगी।

vi. एनसीवीईटी यह सुनिश्चित करने के लिए उत्तरदायी होगा कि किसी कर्मचारी के अलग होने से पहले सभी जारी की गई परिसंपत्ति वापस कर दी गई है और अलग होने पर सभी अकाउंट को निष्क्रिय कर दिया गया है और तुरंत पहुंच (एक्सेस) को हटा दिया जाए।

8.10 सुरक्षा और घटना प्रबंधन

i. एनसीवीईटी द्वारा सुरक्षा घटनाओं पर प्रभावी ढंग से प्रतिक्रिया देने के लिए एक घटना प्रतिक्रिया योजना, सुसंगत मानक बनाई जाएगी।

ii. सभी ज्ञात अथवा संदिग्ध सूचना सुरक्षा घटनाओं या संवेदनशीलताओं की रिपोर्ट उचित प्रबंधन और सीआईएसओ/ नामित सुरक्षा प्रतिनिधि को यथाशीघ्र की जाए। यदि कार्यबल के किसी सदस्य को यह लगता है कि साइबर सुरक्षा संबंधी चिंताओं को उचित तरीके से संबोधित नहीं किया जा रहा है, तो वह खतरे की रिपोर्ट करने के लिए गोपनीय रूप से सीधे एनसीवीईटी के अध्यक्ष से संपर्क कर सकते हैं।

iii. सुरक्षा प्रचालन केंद्र/ सीईआरटी-इन को ऐसी किसी भी साइबर घटना के बारे में सूचित किया जाए, जिसका प्रचालन या सुरक्षा पर महत्वपूर्ण या गंभीर प्रभाव पड़ सकता हो या जिसमें डिजिटल फोरेंसिक शामिल है, ताकि उचित घटना प्रतिक्रिया प्रक्रियाओं का पालन किया जा सके और समन्वयन तथा निगरानी की गारंटी दी जा सके।

8.11. आईटी परिसंपत्ति प्रबंधन

i. सभी आईटी हार्डवेयर और सॉफ्टवेयर परिसंपत्तियों को एक निर्दिष्ट संगठनात्मक इकाई अथवा व्यक्ति को सौंपा जाए।

ii. एनसीवीईटी हार्डवेयर और सॉफ्टवेयर परिसंपत्तियों की एक सूची का रखरखाव करेगा, जिसमें सभी सिस्टम घटक (जैसे नेटवर्क, पता, मशीन का नाम, सॉफ्टेवेयर संस्करण) शामिल हैं, जो ट्रेकिंग और रिपोर्टिंग के लिए आवश्यक समझे जाने वाले ग्रेन्युलेरिटी के स्तर पर हैं। यह वस्तुसूची जहां तकनीकी रूप से संभव हो, स्वचालित की जा सकती है।

iii. अनधिकृत हार्डवेयर और/ अथवा सॉफ्टवेयर की पहचान करने और पता चलने पर उपयुक्त कर्मचारियों को सूचित करने के लिए नियमित स्कैनिंग सहित प्रक्रियाओं को लागू किया जाना चाहिए।

8.12. मोबिलिटी और अपना स्वयं का उपकरण लाएं (बीवाईओडी)

i. विशिष्ट व्यक्ति एनसीवीईटी के डेटा और सिस्टम को अपने एक्सेस अधिकारों और विशेषाधिकारों के रूप में एक्सेस कर सकते हैं, जो उनके या उनके संबंधित संगठनों के स्वामित्व वाले/ प्रबंधित ऐंड प्वाइंट कंप्यूटिंग डिवाइस हैं।

ii. ये डिवाइस निकनेट के एसओपी में उल्लिखित सभी सॉफ्टवेयर और उपकरणों के मानकों का अनुपालन करेंगे।

iii. प्रयोक्ताओं को एनसीवीईटी पासवर्ड नीति या बायोमेट्रिक के अनुसार सुरक्षित पासवर्ड के साथ डिवाइस को कांफिगर करना होगा।

iv. नीति का अनुपालन सुनिश्चित करने के लिए एनसीवीईटी समय-समय पर मोबाइल और प्रयोक्ता के स्वामित्व वाले उपकरणों की ऑडिट करेगा।

v. अतिथियों के लिए निकनेट का उपयोग:

अतिथियों को वाईफाई स्वागत के माध्यम से निकनेट का उपयोग प्रदान किया जाएगा। स्वागत टीम कौशल भवन समन्वयक के साथ दैनिक रूप से ओटीपी भेजती है, जिसे आईटी सहायता टीम के साथ साझा किया जाएगा। आईवाईटी सपोर्ट टीम बदले में ओटीपी को अतिथियों के साथ साझा कर सकती है और उन्हें पंजीकृत करवा सकती है। *(संदर्भः नेटवर्क सुरक्षा के लिए एसओपी, एमएसडीई)*

8.13. आधिकारिक सोशल मीडिया अकाउंट के लिए सुरक्षा उपाय

i. आधिकारिक सोशल मीडिया अकाउंट के लिए एक्सेस केवल निर्दिष्ट अधिकारियों और प्रणालियों के लिए ही दिया जाएगा।

ii. प्रत्येक सोशल मीडिया अकाउंट प्लेटफार्म एक समर्पित और पृथक ईमेल अकाउंट का उपयोग करके संचालित किया जाएगा।

iii. आधिकारिक ईमेल अकाउंट और सोशल मीडिया प्लेटफार्म अकाउंट के लिए अलग क्रेडेंशियल सेट होगा।

iv. सभी सोशल मीडिया अकाउंट प्लेटफार्म अकाउंट क्रेडेंशियल द्वारा संगठन की पासवर्ड नीति का अनुसरण किया जाएगा।

v. निजी ईमेल अकाउंट का उपयोग प्रचालनीय आधिकारिक सोशल मीडिया अकाउंट के लिए किया जाना चाहिए।

vi. मल्टी फेक्टर प्रमाणीकरण (एमएफए) को जहां कहीं भी संभव हो, सभी सोशल मीडिया अकाउंट के लिए सक्षम किया जाएगा।

vii. सोशल मीडिया हैंडल पर डाली गई समस्त सामग्री के लिए संगठन के भीतर एक उपयुक्त प्राधिकारी द्वारा अनुमोदन अपेक्षित है।

viii. आधिकारिक सोशल मीडिया अकाउंट केवल निर्दिष्ट अधिकारियों द्वारा और विश्वसनीय उपकरणों पर संचालित किया जाएगा।

ix. यूजर द्वारा उपयोग करने के तुरंत बाद आधिकारिक सोशल मीडिया प्लेटफार्म अकाउंट से लॉगआउट किया जाए।

x. आधिकारिक सोशल मीडिया प्लेटफार्म अकाउंट का प्रयोग सार्वजनिक अथवा अनधिकृत उपकरणों पर नहीं किया जाएगा।

xi. आधिकारिक सोशल मीडिया प्लेटफार्म के लिए/ जियोलोकेशन (जीपीएस) एक्सेस विशेषताएं अक्षम (डिसेबल) की जाएगी।

xii. सोशल मीडिया प्लेटफार्म सॉफ्टवेयर/ एप्लिकेशन को नवीनतम संस्करण (वर्सन) पर अपलोड किया जाए और आधिकारिक सोशल मीडिया अकाउंट का संचालन करने वाले उपकरणों को नवीनतम उपलब्ध सुरक्षा पैच के साथ अद्यतन किया जाएगा।

xiii. सोशल मीडिया कंपनियों द्वारा सुरक्षा और निजता की सेटिगं के बारे में हमेशा सूचित किया जाए और उन्हें उपयुक्त रूप से कार्यान्वित किया जाए।

xiv. सोशल मीडिया प्रबंधन प्लेटफार्म और आधिकारिक सोशल मीडिया अकाउंट के लिए उपयुक्त विशेषाधिकार के साथ भूमिका आधारित अकाउंट सक्षम किया जाएगा।

xv. जब कर्मचारी की भूमिका बदलती है अथवा कर्मचारी संगठन को छोड़ता है तो आधिकारिक सोशल मीडिया अकाउंट के लिए एक्सेस हटा ली जाएगी।

xvi. अकाउंट सुरक्षा लॉग सक्षम किए जाएंगे और उनकी आवधिक निगरानी की जाएगी ताकि अविश्वसनीय. उपकरणों अथवा नियमित क्षेत्रों से इतर क्षेत्रों से लॉगिन के प्रयास की पहचान की जा सके।

xvii. अमान्य लॉगिन प्रयासों के लिए सोशल मीडिया प्लेटफार्म की लॉगिन और सुरक्षा सेटिंग के अंतर्गत चेतावनी (अलर्ट) सक्षम की जाए।

xviii. सोशल मीडिया प्लेटफार्म अकाउंट के प्रबंधन के लिए थर्ड पार्टी एप्लिकेशन का उपयोग करते समय चेतावनी का प्रयोग किया जाए।

xix. आधिकारिक सोशल मीडिया अकाउंट के साथ जुड़े ईमेल अकाउंट की किसी भी अकाउंट गतिविधि अलर्ट के लिए नियमित रूप से निगरानी की जाए।

8.14. सुरक्षा परीक्षण/ऑडिट

i. एनसीवीईटी सभी प्रणालियों, अनुप्रयोगों, नेटवर्क, नीतियों, प्रक्रियाओं और प्रौद्योगिकी प्लेटफार्म जैसे क्लाउड कम्प्यूटरिंग, मोबिलिटी प्लेटफार्म, वर्चुअल परिवेश आदि का मूल्यांकन करने के लिए सुरक्षा परीक्षण आयोजित करेगा, ताकि सीईआरटी-इन दिशानिर्देशों के अनुसार सुभेद्यता की पहचान की जा सके।

ii. एनसीवीईटी आंतरिक और बाहरी जोखिम एजेंट वाले परिदृश्य का निर्माण करके सुरक्षा मूल्यांकन करेगा।

iii. एनसीवीईटी थर्ड पार्टी द्वारा प्रबंधित सिस्टम सहित अपने परिनियोजित/ स्वामित्व वाले सिस्टम पर नीचे दिए गए मापदंडों के आधार पर सुरक्षा जांच अपेक्षाओं का निर्धारण और वर्णन करेगा:

   क. प्रचालनों की प्रकृति, संगठनों की जोखिम प्रवृत्ति, प्रक्रियाओं और प्रचालन सौदों की महत्वपूर्णता
   ख. सुरक्षा जोखिमों के लिए संगठनात्मक सूचना का प्रकटन
   ग. उद्यम सुरक्षा नीति, रणनीति और मानक
   घ. कानूनी और अनुपालन अपेक्षाएं
   ड. ऐतिहासिक सूचना, विगत जांच रिपोर्ट, सुरक्षा घटनाएं

iv. एनसीवीईटी सभी सूचना प्रणालियों, अवसंरचना सुविधाओं, थर्ड पार्टी आदि की आवधिक ऑडिट करेगा, जो वर्गीकृत डेटा का उसके जीवन चक्र में किसी घटना का संचालन करता है।

ii. सुरक्षा जांच एक स्वतंत्र थर्ड पार्टी द्वारा की जाएगी, जिसमें सुरक्षा जांच (ऑडिट) करने के लिए आवश्यक कौशल के साथ एक समर्पित टीम होगी।

iii. एनसीवीईटी यह सुनिश्चित करेगा कि ऑडिट टीम द्वारा सभी ऑडिट अवलोकन, मुद्दें और सिफारिशें निर्दिष्ट कार्मिकों को बताई जाती हैं और एक आवश्यक समयबद्ध तरीके में समाधान और सुधार किया जाता है।

8.15. प्रचालनों की सुरक्षा

i. सभी प्रणालियों और भौतिक सुविधाओं में, जिनमें उन्हें स्टोर किया जाता है, दस्तावेजी प्रचालन निर्देश, प्रबंधन कार्यविधियां और सूचना सुरक्षा मामलों संबंधी औपचारिक घटना प्रबंधन कार्यविधियां होनी चाहिए, जो उनका प्रचालन करने वाले अथवा उनका प्रयोग करने वाले प्रभावित व्यक्तियों की भूमिकाओं और उत्तरदायित्वों को परिभाषित करती हैं।

ii. सिस्टम कॉफिगुरेशन द्वारा अनुमोदित कॉफिगुरेसन मानकों का अनुसरण किया जाए।

iii. अग्रिम योजना और नियोजन किए जाने चाहिए, ताकि पर्याप्त क्षमता और संसाधनों की उपलब्धता सुनिश्चित की जा सके। प्रणाली की क्षमता की निगरानी निरंतर आधार पर की जानी चाहिए।

iv. जहां एनसीवीईटी किसी अन्य संस्था को एक सर्वर, एप्लिकेशन अथवा नेटवर्क सेवा प्रदान करता है, प्रचालन और प्रबंधन उत्तरदायित्वों को सभी प्रभावित संस्थाओं द्वारा समन्वित किया जाए।

v. होस्ट आधारित फायरवाल लगाए जाएं और सभी कार्यस्थलों पर सक्षम किए जाएं ताकि जोखिमों से संरक्षण हो सके और इसे केवल जरूरतमंद तक ही सीमित किया जाए।

vi. सभी सिस्टम पर नियंत्रण लागू किए जाएं (अर्थात एंटी-वायरस, सॉफ्टवेयर प्रामाणिकता, जांचकर्ता, वेब फिल्टरिंग), जहां तकनीकी रूप से व्यवहारिक हो ताकि हानिकारक कोड अथवा अन्य जोखिमों को रोका जा सके और उसका पता लगाया जा सके।

vii. हटाने योग्य मीडिया से सामग्री के स्वचालित (ऑटोमेटेड) निष्पादन को अक्षम (डिसेबल) करने के लिए नियंत्रण लागू किया जाना चाहिए।

viii. अधिकृत स्थानों तक सूचना के भंडारण को सीमित करने के लिए नियंत्रणों को लागू किया जाए।

ix. एक सिस्टम पर केवल अनुमोदित सॉफ्टवेयर को चलाने के लिए और सभी अन्य सॉफ्टवेयर का निष्पादन रोकने के लिए ही अनुमति हेतु नियंत्रण लागू किए जाएं।

x. सभी सिस्टम को एक वेंडर सहायता प्राप्त स्तर पर रखा जाए ताकि सटीकता और प्रामाणिकता सुनिश्चित हो सके।

xi. सभी सुरक्षा पैच की एक समयबद्ध ढंग से समीक्षा की जाए, मूल्यांकन किया जाए और उपयुक्त रूप से लागू किया जाए। यह प्रक्रिया जहां तक तकनीकी रूप से संभव हो, ऑटोमेटेड होनी चाहिए।

xii. जिन सिस्टम की अब आगे सहायता नहीं की जा सकती अथवा वर्तमान संस्करणों के लिए पैच नहीं किया जा सकता, उन्हें हटा लिया जाए।

xiii. सिस्टम और एप्लिकेशन की निगरानी और विश्लेषण किया जाए ताकि इस नीति और सुरक्षा लॉगिंक मानक में उल्लिखित एक्सेस नियंत्रण अपेक्षाओं से विचलन का पता लगाया जा सके और साक्ष्य प्रदान करने के लिए तथा खोए और क्षतिग्रस्त डेटा के पुनर्निर्माण के लिए घटनाओं को रिकार्ड किया जा सके।

xiv. ऑडिट लॉग रिकार्डिंग अपवादों और अन्य सुरक्षा संबंधी घटनाओं का रिकार्ड रखने की अनुसूची तथा अपेक्षाओं के अनुसार उत्पादन, संरक्षण और रखरखाव किया जाए।

xv. कार्यनीतिक स्थानों पर निगरानी प्रणालियां लगाई जाए (अर्थात घुसपैठ का पता लगाना/ संरक्षण प्रणालियां) ताकि लागू कारोबारी मानदंड पर इनबाउंड, आउटबाउंड और आंतरिक नेटवर्क ट्रेफिक की निगरानी की जा सके।

xvi. निगरानी प्रणालियों को कॉफिगर किया जाए ताकि समझौता अथवा संभावित समझौता के संकेतकों के लिए घटना प्रतिक्रिया कार्मिकों को अलर्ट किया जा सके।

xvii. एनसीवीईटी सूचना, सॉफ्टवेयर और प्रणाली इमेज की बैकअप प्रतियां एनसीवीईटी की परिभाषित अपेक्षाओं के अनुसार नियमित रूप से प्राप्त की जाए।

xviii. बैकअप और रेस्टोरेशन का नियमित परीक्षण किया जाए। कर्त्तव्यों का विभाजन इन कार्यों के लिए लागू किया जाए।

xix. किसी प्रतिकूल घटना के दौरान सूचना सुरक्षा के रखरखाव के लिए कार्यविधियां स्थापित की जाए। उन नियंत्रणों के लिए, जिन्हें बनाए नहीं रखा जा सकता, प्रतिपूरक नियंत्रण लागू किए जाए।

8.16. आकस्मिक योजना

आकस्मिक योजनाएं (अर्थात कारोबारी निरंतरता योजनाएं, आपदा बहाली योजनाएं, प्रचालन योजनाओं की निरंतरता) स्थापित की जाए और नियमित रूप से परीक्षण किया जाए।

क. सूचना प्रसंस्करण (सॉफ्टवेयर और प्रचालन प्रणालियों, फायरवाल, स्विच, राउटर और अन्य संचार उपकरण शामिल किंतु ये इन्हीं तक सीमित नहीं हैं) में प्रयुक्त प्रणालियों के महत्व का मूल्यांकन

ख. सभी महत्वपूर्ण प्रणालियों के लिए रिकवरी समय उद्देश्य (आरटीओ)/ रिकवरी प्वाइंट उद्देश्य (आरपीओ)

9. अनुपालन विवरण

यह दिशानिर्देश अधिसूचित किए जाने पर प्रभावी होगा। सभी उद्यम नीतियों और मानकों का अनुपालन अपेक्षित है। नीतियों और मानकों को किसी भी समय संशोधित किया जा सकता है; संशोधित नीतियों और मानकों का अनुपालन अपेक्षित है।

यदि इस मानक का अनुपालन व्यवहार्य या तकनीकी रूप से संभव नहीं है, या यदि किसी व्यावसायिक कार्य को समर्थन देने के लिए इस नीति से विचलन आवश्यक है, तो संस्थाएँ प्रौद्योगिकी सूचना सुरक्षा अधिकारी (सीआईएसओ) अपवाद प्रक्रिया के माध्यम से अपवाद का अनुरोध करेंगी।

एनआईसी/ सीईआरटी-इन के कोई अन्य परामर्श, यदि इस दस्तावेज का हिस्सा नहीं हों, तो भी, उनपर तत्काल कार्रवाई और उनका पालन किया जाना अपेक्षित है।

10. प्रमुख शब्दों की परिभाषाएं

शब्द	परिभाषा
सीआईएसओ	मुख्य सूचना सुरक्षा अधिकारी
सीईओ	मुख्य कार्यकारी अधिकारी
पीपीआई	प्रीपेड भुगतान साधन
सीईआरटी-ईन	भारतीय कंप्यूटर आकस्मिक प्रतिक्रिया टीम
ओएस	प्रचालन प्रणाली
पीआईआई	निजी पहचान योग्य सूचना
आईएसओ	अंतर्राष्ट्रीय मानकीकरण संगठन
वीपीएन	वर्चुअल प्राइवेट नेटवर्क

11. संदर्भ

1. राष्ट्रीय सूचना सुरक्षा नीति और दिशानिर्देश, गृह मंत्रालय, भारत सरकार, संस्करण 5.0

2. आईएसओ/ आईईसी 27001:2022 (आईएसओ 27001) मानक

   i. संवर्धित जोखिम प्रबंधन फ्रेमवर्क

   ii. सूचना सुरक्षा नीतियां और दस्तावेजीकरण

   iii. प्रौद्योगिकी और जोखिम भूदृश्य अंगीकरण

   iv. सुरक्षित प्रणाली विकास जीवन चक्र (एसएसडीएलसी) मानक

   v. सूचना वर्गीकरण मानक, स्वच्छ/ सुरक्षित निपटान मानक

   vi. सुरक्षित कॉफिगुरेशन मानक

   vii. अकाउंट प्रबंधन/ एक्सेस नियंत्रण मानक

   viii. साइबर घटना प्रतिक्रिया मानक

   ix. प्रमाणीकरण टोकन मानक

   x. रिमोट एक्सेस मानक, सुरक्षा लॉगिंग मानक

   xi. सुरक्षा लॉगिंग मानक

   xii. सुरक्षा कोडिंग मानक

   xiii. सुरक्षा कांफिगुरेशन प्रबंधन मानक

3. राष्ट्रीय मानक और प्रौद्योगिकी संस्थान (एनआईएसटी)- राष्ट्रीय मानक और प्रौद्योगिकी संस्थान (एनआईएसटी) विशेष प्रकाशन 800-53, संघीय सूचना प्रणालियों और संगठनों के लिए सुरक्षा और निजता नियंत्रण।