आईआरडीएआई/आईटी/जीडीएल/विविध/082/04/2017 दिनांक 07/04/2017

प्रति,
सभी बीमाकर्ता

विषयः बीमाकर्ताओं के लिए सूचना और साइबर सुरक्षा संबंधी दिशानिर्देश

बीमा क्षेत्र के लिए व्यापक सूचना और साइबर सुरक्षा ढाँचे के निर्माण संबंधी आईआरडीएआई के परिपत्र सं. आईआरडीए/आईटी/सीआईआर/विविध/216/10/2016 दिनांक 31 अक्तूबर 2016 की ओर ध्यान आकर्षित किया जाता है। परिणामस्वरूप, सूचना और साइबर सुरक्षा हेतु एक व्यापक ढाँचा प्राप्त करने के लिए बीमा कंपनियों से लिये गये विशेषज्ञों से युक्त निम्नलिखित उप-समूह बनाये गये थेः
समूह-1 : सुरक्षा के सभी चार स्तर (डेटा, अनुप्रयोग, परिचालन प्रणाली और नेटवर्क स्तर)
समूह-2 : सुरक्षा संपरीक्षण
समूह-3 : साइबर सुरक्षा संबंधी कानूनी पहलू

आईआरडीएआई ने उक्त प्रारूप से युक्त एक्सपोज़र प्रारूप 2 मार्च 2017 को जारी किया। उक्त एक्सपोज़र प्रारूप के प्रति हितधारकों से प्राप्त प्रतिसूचना (फीडबैक) पर विचार करते हुए, आईआरडीएआई अब आईआरडीए अधिनियम, 1999 की धारा 14 की उप-धारा (1) के अंतर्गत प्राधिकरण के पास निहित शक्तियों का प्रयोग करते हुए संलग्न `बीमाकर्ताओं के लिए सूचना और साइबर सुरक्षा संबंधी दिशानिर्देश' जारी करता है।

इन दिशानिर्देशों के प्रभावी कार्यान्वयन के लिए एक विस्तृत नियंत्रण जाँच-सूची **अनुबंध क** के अनुसार संलग्न है।

ये दिशानिर्देश सभी बीमाकर्ताओं के लिए लागू हैं। मध्यवर्तियों औऱ अन्य विनियमित संस्थाओं के मामले में, जिनके साथ पालिसीधारक संबंधी सूचना की साझेदारी की जाती है, यह सुनिश्चित करने के लिए बीमाकर्ताओं का दायित्व होगा कि पर्याप्त व्यवस्थाएँ लागू हों, जिससे यह सुनिश्चित किया जा सके कि सूचना और साइबर सुरक्षा संबंधी समस्याओं का समाधान किया जाए। जिन बीमाकर्ताओं ने व्यवसाय प्रारंभ करने की तारीख से तीन वर्ष पूरे नहीं किये हैं, उन्हें मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) के रूप में एक पूर्णकालिक व्यक्ति की नियुक्ति करने की अपेक्षा से छूट दी गई है। तथापि, सीआईएसओ का दायित्व

का ध्यान बोर्ड को रिपोर्ट करनेवाले किसी भी पदाधिकारी द्वारा रखा जा सकता है। दिशानिर्देशों के दस्तावेज में निर्धारित सभी अन्य अपेक्षाएँ इन बीमाकर्ताओं पर लागू होंगे।

कार्यान्वयन के लिए समय-सीमाएँ

1	एकमात्र तौर पर मुख्य सूचना सुरक्षा अधिकारी (सीएसआईओ) के रूप में एक उपयुक्त रूप में अर्हता-प्राप्त और अनुभवी वरिष्ठ स्तर के अधिकारी की नियुक्ति/मनोनयन, जो उनकी सूचना परिसंपत्तियों का संरक्षण करने के लिए नीतियों को स्पष्ट रूप से व्यक्त करने और प्रवर्तित करने तथा सूचना सुरक्षा समिति (आईएससी) के गठन के लिए उत्तरदायी होगा।	30 अप्रैल 2017
2	अंतराल विश्लेषण रिपोर्ट (दिशानिर्देशों के इस दस्तावेज में बताई गई अपेक्षाओं की तुलना में एएस-आईएस) तैयार करना	30 जून 2017
3	साइबर संकट प्रबंध योजना बनाना	30 जून 2017
4	बोर्ड द्वारा अनुमोदित सूचना और साइबर सुरक्षा नीति को अंतिम रूप देना	31 जुलाई 2017
5	बोर्ड द्वारा अनुमोदित सूचना और साइबर सुरक्षा नीति के अनुरूप सूचना और साइबर सुरक्षा बीमा कार्यक्रम (कार्यान्वयन योजना / दिशानिर्देश) बनाना	30 सितंबर 2017
6	प्रथम व्यापक सूचना और साइबर सुरक्षा बीमा संपरीक्षण का समापन	31 मार्च 2018

बीमाकर्ताओं से प्रत्याशित है कि वे उपर्युक्त समय-सीमाओं के अनुसार 31 मार्च 2018 तक पूर्णतः अनुपालनकर्ता होने के लिए उपयुक्त कदम उठाएँ। अध्याय सं. 23 के अंतर्गत निर्धारित रूप में पहली संपरीक्षण रिपोर्ट आईआरडीएआई को 31 मार्च 2018 तक प्रस्तुत की जाएगी। ऊपर क्रम सं. 1 - 5 में बताई गई गतिविधियाँ समांतर रूप से संचालित की जाएँ ताकि यह सुनिश्चित किया जा सके कि इन्हें निर्धारित समय-सीमाओं में पूरा किया जा सके।

हस्ता./-

नीलेश साठे

सदस्य (जीवन)

बीमाकर्ताओं के लिए
सूचना और साइबर सुरक्षा संबंधी दिशानिर्देश

भारतीय बीमा विनियामक और विकास प्राधिकरण (आईआरडीएआई)

विषय-सूची

10.3 व्यवसाय निरंतरता और संकट समुत्थान

11. डेटा सुरक्षा

11.1 डेटा सुरक्षा नीति की योजना

12. अनुप्रयोग सुरक्षा

12.1 प्रत्येक अनुप्रयोग का स्वामी होगा

12.2 सूचना सुरक्षा अपेक्षाओं का विश्लेषण और विशेष विवरण

12.3 परिचालन प्लेटफार्म परिवर्तनों के बाद अनुप्रयोगों की तकनीकी समीक्षा

12.4 सुरक्षा प्रणाली अभियांत्रिकी सिद्धांत

12.5 सुरक्षित विकास पर्यावरण

12.6 बाह्यस्रोतीकृत विकास

12.7 प्रणाली कार्यात्मकता और सुरक्षा परीक्षण

12.8 अन्य

13. साइबर सुरक्षा

13.1 संकटपूर्ण प्रणालियों और साइबर सुरक्षा घटनाओँ का वर्गीकरण

13.2 संस्था का साइबर आघात-सहनीयता कार्यक्रम

13.3 अभिनिर्धारण

13.4 संरक्षण

13.5 पहचान

13.6 प्रतिक्रिया और पुनःप्राप्ति

13.7 परीक्षण

13.8 परिस्थितिगत जागरूकता

13.9 जानकारी और प्रतिवेदन

14.**प्लेटफार्म/बुनियादी व्यवस्था की सुरक्षा**

14.1 सुरक्षित विन्यासदस्तावेज और आवधिक निर्धारण

14.2 संग्रथन प्रबंध

15. नेटवर्क सुरक्षा

16. बीज-लेखन और कुंजी प्रबंध

16.1 कुंजियों संबंधी सामान्य निदेश

16.2 इलेक्ट्रानिक कुंजियों का प्रतिधारण

17. सुरक्षा लागिंग और निगरानी

17.1 लागिंग और निगरानी

18. घटना प्रबंध

18.1 घटना का प्रतिवेदन तथा उन्नयन सँभलाई प्रक्रियाएँ और क्रियाविधियाँ

18.2 निवारक और अभिज्ञापक नियंत्रणों की कार्यपद्धति की समीक्षा

19.अंतिम स्थान (एण्ड पाइण्ट) सुरक्षा

19.1 वस्तुनिष्ठ अंतिम स्थान सुरक्षा

19.2 पहचान और अंतिम स्थानों पर प्रवेश

19.3 नेटवर्क प्रवेश नियंत्रण

19.4 दूरस्थ प्रवेश

19.5 अनुप्रयोग नियंत्रण

19.6 साधन नियंत्रण

20. आभासीकरण

20.1 प्रवेश नियंत्रण

20.2 परिचालन प्रणालियों का कठोरीकरण

20.3 विभाजन और संसाधन आबंटन

20.4 फाइल साझेदारी

20.5 बैक अप

20.6 निगरानी

21. क्लाउड सुरक्षा

21.1 सेवा स्तरीय करार

21.2 क्लाउड प्रवेश नियंत्रण

21.3 क्लाउड डेटा सुरक्षा

22. गतिशील सुरक्षा

22.1 अनुमोदित साधन/सेवाएँ

22.2 घटना प्रबंध

22.3 दूरस्थ अवरोधन और दूरस्थ प्रहार

22.4 नेटवर्क प्रवेश नियंत्रण

22.5 गतिशील डेटा सुरक्षा

23. सूचना प्रणाली संपरीक्षण

23.1 संपरीक्षक की पात्रता औऱ चयन

23.2 संपरीक्षण का विस्तार/प्रकार

23.3 आवृत्ति

23.4 आईएस संपरीक्षण का निष्पादन

23.5 रिपर्टिंग और अनुवर्ती कार्रवाइयाँ

23.6 समीक्षा

24.**सूचना और साइबर सुरक्षा संबंधी कानूनी संदर्भ**

अनुबंध खः सूचना और साइबर सुरक्षा के लिए कानूनी संदर्भ

1. प्रस्तावना

आकार, जटिलता, अथवा व्यवसाय की व्यवस्थाओं का विचार किये बिना सभी बीमाकर्ता विभिन्न अन्य पक्षकारों (उदा. सेवा प्रदाताओँ, पुनर्बीमाकर्ताओँ आदि) के साथ कुछ उदाहरणों में संवेदनशील स्वास्थ्य-संबंधी सूचना सहित, वैयक्तिक और गोपनीय पालिसीधारक संबंधी सूचना की विपुल मात्राओँ में साझेदारी करते हैं।

बीमा भंडार (रिपोजिटरियाँ), काल सेंटर, सामान्य सेवा केन्द्र आदि में भी पालिसीधारकों के डेटा तक पहुँच उपलब्ध है।

जबकि व्यवसाय के परिचालन संचालित करने के लिए सूचना की साझेदारी अत्यंत आवश्यक है, यह सुनिश्चित करना अत्यावश्यक है कि यह सुनिश्चित करने के लिए पर्याप्त प्रणालियाँ और प्रक्रियाएँ लागू हों कि सूचना का प्रकटन न हो तथा सूचना की साझेदारी केवल जानने की आवश्यकता के आधार पर ही की जाए।

इसके अलावा, सूचना प्रौद्योगिकी के तीव्र विकास के कारण, सूचना की गोपनीयता का बनाये रखने में अनेक चुनौतियाँ हैं। इस प्रौद्योगिकी के यद्यपि अनेक लाभ हैं, तथापि यह किसी अन्य प्रौद्योगिकी की तरह ही अपने साथ जोखिम संबद्ध किये हुए है। वेब आधारित अनुप्रयोगों की तीव्र वृद्धि के साथ ही, साइबर आशंका के परिदृश्य की वृद्धि हो रही है तथा इस विषय में सभी क्षेत्रों में चिंता है।साइबर जोखिम बढ़ गये हैं और साइबर अपराधी अधिकाधिक परिष्कृत बन गये हैं।बीमाकर्ताओं के लिए, साइबर सुरक्षा संबंधी घटनाएँ व्यवसाय को चलाने की क्षमता को हानि पहुँचा सकती हैं, वैयक्तिक और स्वामित्व डेटा के संरक्षण को संकट में डाल सकती हैं, तथा इस क्षेत्र में विश्वास को नष्ट कर सकती हैं। यह पाया गया है कि बीमा क्षेत्र के अंदर साइबर आशंकाओँ और साइबर सुरक्षा के संबंध में जागरूकता के स्तर एवं उक्त जोखिमों का सामना करने के प्रति पर्यवेक्षी दृष्टिकोण सभी संस्थाओँ के बीच भिन्न-भिन्न प्रतीत होते हैं।

साइबर अपराध के द्वारा विनियमित संस्थाओँ से प्राप्त सूचना का उपयोग तोड़-मरोड़, पहचान की चोरी, बौद्धिक संपत्ति के दुर्विनियोजन, अथवा अन्य आपराधिक कार्यकलापों के जरिये वित्तीय लाभ के लिए किया जा सकता है। वैयक्तिक डेटा का प्रकटीकरण संभावित रूप

से प्रभावित पालिसीधारकों के लिए तीव्र हानि में परिणत हो सकता है, एवं बीमा क्षेत्र के सहभागियों को प्रतिष्ठागत क्षति पहुँचा सकता है। इसी प्रकार, बीमाकर्ता और बीमा मध्यवर्तियों की महत्वपूर्ण प्रणालियों के विरुद्ध दुर्भावपूर्ण आक्रमण व्यवसाय संचालित करने की उनकी क्षमता को बाधित कर सकते हैं।

सुरक्षा से संबंधित ऐसी समस्याएँ जनता के विश्वास को दुर्बल बनाने की संभाव्यता से युक्त हैं तथा बीमाकर्ताओँ हेतु प्रतिष्ठागत जोखिम के लिए मार्ग प्रशस्त कर सकती हैं। अतः यह सुनिश्चित करना अत्यावश्यक है कि बीमाकर्ताओं के लिए सूचना और साइबर सुरक्षा हेतु एक समरूप ढाँचा कार्यान्वित किया जाए तथा विनियमित संस्थाओँ के अंदर एक अंतर्निहित अभिशासन व्यवस्था लागू की जाए जिससे यह सुनिश्चित किया जा सके कि समय-समय पर सुरक्षा से संबंधित ऐसी समस्याओँ का समाधान किया जाए।

2. परिदृष्टि और उद्देश्य

(i) यह सुनिश्चित करना कि सभी बीमाकर्ताओं के पास बोर्ड द्वारा अनुमोदित सूचना और साइबर सुरक्षा नीति विद्यमान हो।

(ii) यह सुनिश्चित करना कि सूचना और साइबर सुरक्षा संबंधी विषयों के लिए बीमाकर्ताओं द्वारा आवश्यक कार्यान्वयन प्रक्रियाएँ निर्धारित की जाएँ।

(iii) यह सुनिश्चित करना कि बीमाकर्ता सूचना और साइबर सुरक्षा संबंधी जोखिम कम करने के लिए पर्याप्त रूप से तैयार हों।

(iv) यह सुनिश्चित करना कि सूचना और साइबर सुरक्षा ढाँचे के प्रभावी कार्यान्वयन के लिए एक अंतर्निहित अभिशासन व्यवस्था विद्यमान हो।

3. प्रयोज्यता

यह दिशानिर्देश दस्तावेज भारतीय बीमा विनियामक और विकास प्राधिकरण (आईआरडीएआई) द्वारा विनियमित सभी बीमाकर्ताओं के लिए लागू है।

ये दिशानिर्देश बीमाकर्ताओं द्वारा अपने निर्दिष्ट कर्तव्यों और कार्यों का निर्वहण करने के दौरान निर्मित, प्राप्त अथवा अनुरक्षित समस्त डेटा पर लागू हैं चाहे ये डेटा अभिलेख जहाँ कहीं भी हों तथा किसी भी रूप में हों।

`नियंत्रण जाँच-सूची'**अनुबंध क** में दी गई है।

4. शब्द और परिभाषाएँ

एडीएमआईएन (अडमिन)	प्रशासन
बीसीएम/बीसीपी--	व्यवसाय निरंतरता प्रबंध/योजना
बीवाईओडी	अपना स्वयं का साधन लाएँ
सीए	प्रमाणन अधिकारी
सीसीए	प्रमाणीकरण प्राधिकरण का नियंत्रक
सीईआरटी आईएन	कंप्यूटर आपाती प्रतिक्रिया दल - भारत
सीसीएमपी	व्यापक साइबर संकट प्रबंध योजना
सीआईओ	मुख्य सूचना अधिकारी
सीआईए	गोपनीयता, सत्यनिष्ठा और उपलब्धता
सीआईएसए	प्रमाणित सूचना प्रणाली संपरीक्षक
सीआईएसओ	मुख्य सूचना सुरक्षा अधिकारी
सीआरओ	मुख्य जोखिम अधिकारी
डीडीओएस	सेवा की वितरित अस्वीकृति
डीआईएसए	सूचना प्रणाली संपरीक्षण में डिप्लोमा
डीएलपी	डेटा हानि निवारण
डीआर	आपदा उद्धार
एचआर	मानव संसाधन
आईडीएस	अतिक्रमी पहचान प्रणाली
आईएमईआई	अंतरराष्ट्रीय गतिशील उपस्कर पहचान
आईपीएस	अतिक्रमी निवारण प्रणाली
आईआरडीएआई	भारतीय बीमा विनियामक और विकास प्राधिकरण
आईआरएम	सूचना जोखिम प्रबंध
आईएससी	सूचना सुरक्षा समिति
एमएसी	मीडिया प्रवेश नियंत्रण
एनसीआईआईपीसी	राष्ट्रीय महत्वपूर्ण सूचना बुनियादी संरचना संरक्षण केन्द्र
एनडीए	अप्रकटीकरण करार
ओईएम	मूल उपस्कर विनिर्माता
संगठन/संस्था	आईआरडीएआई के पास पंजीकृत बीमा कंपनी
पीआईआई	व्यक्तिगत रूप से पहचानयोग्य सूचना
एससीडी	सुरक्षित विन्यास दस्तावेज
एसएलए	सेवा स्तरीय करार
एसओसी	सुरक्षा परिचालन केन्द्र

एसओपी	मानक परिचालन प्रक्रिया
वीएलएएन	आभासी स्थानीय क्षेत्र नेटवर्क
वीएम	आभासी मशीन
वीपीएन	आभासी निजी नेटवर्क

5. उद्यम सुरक्षा

5.1 अभिशासन, नीति और मानक, कार्यनीति

यह सुनिश्चित करने के लिए कि संस्था की सूचना सुरक्षा का समग्र उद्देश्य प्राप्त किया गया है, संस्था बोर्ड द्वारा अनुमोदित सूचना और साइबर सुरक्षा नीति/नीतियों (इन दिशानिर्देशों में इसके बाद `आईएस नीति' के रूप में उल्लिखित) का अंगीकरण, निदेशन, निगरानी और संचारण करेगी।

5.2 अभिशासन ढाँचे की स्थापना

संस्था द्वारा सूचना सुरक्षा अभिशासन के ढाँचे की स्थापना की जाएगी।

5.3 मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ)

प्रत्येक संस्था एकमात्र तौर पर मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) के रूप में एक उपयुक्त रूप से अर्हता-प्राप्त और अनुभवी वरिष्ठ स्तर के अधिकारी को नियुक्त/ पदनामित करेगी जो उनकी सूचना परिसंपत्तियों का संरक्षण करने के लिए नीतियाँव्यक्त करने और प्रवर्तित करने के लिए जिम्मेदार होगा।

5.4 सीआईएसओ की भूमिकाएँ और दायित्व

क) संस्था के लिए सूचना और साइबर सुरक्षा नीति व्यक्त करने के लिए उत्तरदायी होगा।
ख) सूचना और साइबर सुरक्षा नीति के कार्यान्वयन में प्रबंधक-वर्ग और सूचना के प्रयोक्ताओं को परामर्श और सहायता प्रदान करने के लिए उत्तरदायी होगा।
ग) सूचना सुरक्षा कार्यक्रम को लागू करने के लिए उपयुक्त क्षमताओँ और अभिवृत्ति के साथ सूचना सुरक्षा दल को निर्मित करना और उनका मार्गदर्शन करना।
घ) संस्था के अंदर प्रयोक्ता जागरूकता पहलों को बढ़ावा देना।
ङ) आईएससी को सूचना और साइबर सुरक्षा नीति प्रस्तावित करना, आईएससी और अन्य व्यावसायिक क्षेत्रों से उक्त नीति के निहितार्थों पर प्रतिसूचना (फीडबैक) को नीति-निर्धारक प्रक्रिया में शामिल करना।

च) सूचना और साइबर सुरक्षा नीति के कार्यान्वयन में प्रबंधक-वर्ग और सूचना के प्रयोक्ताओँ को परामर्श और सहायता प्रदान करने के लिए उत्तरदायी होगा।

छ) सूचना सुरक्षा कार्यक्रम को लागू करने के लिए उपयुक्त क्षमताओँ और अभिवृत्ति के साथ सूचना सुरक्षा दल को निर्मित करना और उनका मार्गदर्शन करना।

ज) संस्था के अंदर प्रयोक्ता जागरूकता पहलों को बढ़ावा देना।

सीआईएसओ जोखिम प्रबंधन को रिपोर्ट करेगा तथा आईटी की बुनियादी व्यवस्था और परिचालनों को समझने एवं व्यवसाय की अपेक्षाओँ और उद्देश्यों के अनुरूप समूची संस्था के अंदर आईटी में प्रभावी सुरक्षा निर्मित करने के लिए आवश्यक सौहार्द विकसित करने हेतु सीआईओ के साथ कार्यात्मक संबंध रखेगा। सूचना सुरक्षा और आईटी परिचालनों के लिए संस्था कर्तव्यों का पृथक्करण सुनिश्चित करेगी।

5.5 सूचना सुरक्षा समिति (आईएससी)

सूचना सुरक्षा अभिशासन ढाँचे के लिए समग्र उत्तरदायित्व लेने हेतु संस्था, बोर्ड को रिपोर्टिंग करने की व्यवस्था के साथ वरिष्ठ स्तर के एक कार्यकारी की अध्यक्षता में एक सूचना सुरक्षा समिति (आईएससी) गठित करेगी।

आईएससी के सदस्यों में परिचालन, सूचना प्रौद्योगिकी, विधि, अनुपालन, वित्त, मानव संसाधन, जोखिम आदि विभागों से कार्यात्मक प्रमुख शामिल किये जाएँगे।

उक्त सूचना सुरक्षा समिति (ईएससी) :

क) उच्च स्तरीय आईएस नीति में आवश्यक परिवर्तनों की समीक्षा करेगी और इसके लिए बोर्ड को सिफारिश करेगी। यह समिति बोर्ड द्वारा अनुमोदित आईएस नीति के अनुरूप मानकों और प्रक्रियाओँ का अनुमोदन करेगी। वैयक्तिक व्यावसायिक कार्य निर्मित किये जाएँगे तथा संबंधित कार्यात्मक प्रमुखों के द्वारा उनके एसओपी को (उपर्युक्त मानकों और प्रक्रियाओँ के अनुरूप) अनुमोदित करवाये जाएँगे।

ख) सूचना प्रौद्योगिकी नीति के लिए अपवर्जनों की समीक्षा करेगी, किसी भी उल्लेखनीय जोखिम की सूचना बोर्ड को देगी। तथापि, परिचालन-स्तरीय अपवर्जन सीआईएसओ के साथ परामर्श करने के बाद संबंधित व्यवसाय स्वामी के द्वारा अनुमोदित किये जा सकते हैं।

ग) समिति के संविधान और कार्यपद्धति में परिवर्तनों की सिफारिश करेगी।

घ) सूचना सुरक्षा जोखिम न्यूनीकरण (जिसमें सुरक्षा संबंधी घटनाओँ की रिपोर्टिंग शामिल है) की समीक्षा करेगी, विचार-विमर्श करेगी तथा निर्देशन करेगी एवं सुनिश्चित करेगी कि जोखिम सही तौर पर सूचित किये जाएँ और उपयुक्त रूप में उनके संबंध में कार्रवाई की जाए।

ङ) सूचना प्रौद्योगिकी से संबंधित विनियामक और सांविधिक अपेक्षाओँ का अनुपालन सुनिश्चित करेगी।

च) साइबर सुरक्षा संबंधी पहलुओँका प्रबंध एवं घटना प्रबंध सुनिश्चित करने के लिए उत्तरदायी होगी।

छ) आईएससी यह सुनिश्चित करेगी कि सूचना सुरक्षा अभिशासन ढाँचे का समर्थन एक सूचना सुरक्षा बीमा कार्यक्रम (कार्यान्वयन योजना) के द्वारा किया जाए।

ज) आईएससी को चाहिए कि वर्ष में कम से कम दो बार बोर्ड की जोखिम प्रबंध समिति को रिपोर्ट करे।

झ) सीआईएसओ उक्त सूचना सुरक्षा समिति का संयोजक होगा।

5.6 बोर्ड की भूमिका

बोर्ड निम्नलिखित का अनुमोदन करने के द्वारा अपनी प्रतिबद्धता दर्शायेगाः

- सूचना और साइबर सुरक्षा नीति और कार्यनीति का समग्र ढाँचा।
- सूचना और साइबर सुरक्षा बीमा कार्यक्रम।

5.7 कार्यात्मक विभागों के प्रमुख

प्रत्येक कार्यात्मक प्रमुख सहमत सुरक्षा कार्यक्रम की प्रेरणा अपने प्रबंध के अंतर्गत स्थित दलों को देते हुए और अनुपालन को अधिदेशात्मक करते हुए उक्त सहमत सुरक्षा कार्यक्रम के लिए नेतृत्व और प्रायोजन प्रदान करेगा। वैयक्तिक कार्यात्मक प्रमुख सूचना और साइबर सुरक्षा प्रबंध संबंधी नीतियो के कार्यान्वयन के लिए जिम्मेदार होगा।

5.8 सूचना सुरक्षा दल

संस्थाएँ एकमात्र तौर पर सूचना सुरक्षा प्रबंध पर ध्यान केन्द्रित करने के लिए एक अलग सूचना सुरक्षा दल का गठन करेंगी। केवल सूचना प्रणालियों की सुरक्षा के साथ व्यवहार करनेवाले अधिकारियों के कर्तव्यों का पृथक्करण होना चाहिए तथा सूचना प्रौद्योगिकी प्रभाग

जो वास्तव में सूचना सुरक्षा को कार्यान्वित करता है, परिचालन स्तर पर नियंत्रण करता है। सूचना सुरक्षा कार्य की व्यवस्था संस्था के स्वरूप और कार्यकलापों के आकार के अनुरूप होनी चाहिए। सूचना सुरक्षा दल को स्टाफ की संख्या, कौशल के स्तर तथा जोखिम निर्धारण, सुरक्षा संरचना, असुरक्षितता के निर्धारण, न्यायिक निर्धारण, आदि जैसे उपकरणों अथवा तकनीकों के तौर पर पर्याप्त रूप से संसाधनों से युक्त होना चाहिए। जबकि सूचना सुरक्षा दल, उसके कार्यों और सूचना सुरक्षा अभिशासन संबंधी संरचनाओं का बाह्यस्रोतीकरण (आउटसोर्सिंग) नहीं किया जाना चाहिए, तथापि सूचना सुरक्षा संबंधी विशिष्ट परिचालनात्मक घटकों का बाह्यस्रोतीकरण किया जा सकता है, यदि अपेक्षित संसाधन संस्था के अंदर उपलब्ध न हों। तथापि, अंतिम नियंत्रण और उत्तरदायित्व संस्था के पास स्थित है।

सूचना सुरक्षा दलः -

क) संस्था के सूचना सुरक्षा कार्यक्रम को सहारा देने के लिए आईएस नीति, मानक, प्रक्रियाएँ और दिशानिर्देश विकसित करेगा और उनका अनुरक्षण करेगा।

ख) सूचना सुरक्षा कार्यक्रम को विशिष्ट कार्रवाइयों के रूप में अंतरित करेगा जिनमें जागरूकता, सुरक्षा की बुनियादी संरचना, सुरक्षा घटना प्रतिक्रिया और जोखिम प्रबंध शामिल किये जाएँगे।

ग) आईटी और अन्य कार्यात्मक दलों के साथ घनिष्ठतापूर्वक कार्य करेगा तथा सूचना सुरक्षा परियोजनाओं के कार्यान्वयन की निगरानी करेगा और नई अथवा अभिनिर्धारित कमियों का नियंत्रण करेगा।

घ) सूचना सुरक्षा को प्रभावित करनेवाली वर्तमान और संभावित विधिक और विनियामक समस्याओं का पहचान करेगा तथा विधिक और अनुपालन दल के साथ संयोजन सहित उनके प्रभाव का आकलन करेगा।

ङ) सूचना सुरक्षा संबंधी विषयों के लिए विभिन्न हितधारकों के परामर्शदाताओं और सलाहकारों के रूप में कार्य करेगा।

च) एक निरंतर आधार पर सूचना सुरक्षा जोखिम निर्धारणों का निष्पादन करेगा और किन्हीं महत्वपूर्ण जोखिमों की सूचना आईएससी को देगा।

छ) सूचना सुरक्षा घटना प्रबंध अर्थात् पहचान, प्रतिक्रिया, उपचार और रिपोर्टिंग की निगरानी करेगा।

5.9. कार्यान्वयन

5.9.1 प्रौद्योगिकी/परिचालन/प्रशासन/मानव संसाधन/कार्यात्मक दल-

क) यह सुनिश्चित करने के लिए प्राथमिक दायित्व से युक्त होंगे कि उपयुक्त और पर्याप्त

सुरक्षा व्यवस्थाएँ प्रणालियों में उपलब्ध कराई जाएँगी और नेटवर्क बुनियादी संरचना की साझेदारी सभी प्रणालियों और व्यावसायिक इकाइयों में की जाएगी।

ख) व्यावसायिक स्वामियों के साथ सहमत रूप में बुनियादी संरचना के सभी घटकों के सुरक्षा वर्गीकरण सहमति से युक्त होने के लिए उत्तरदायी होंगे।

ग) विशिष्ट सुरक्षा नीतियों का अनुपालन करने के लिए प्राथमिक स्वामित्व से युक्त होंगे,

जो प्रणालियों के विकास और अधिग्रहण के लिए लागू होगा।

घ) विभिन्न सुरक्षा उपकरणों के अनुरक्षण और समाधानों के लिए उत्तरदायी होंगे।

ङ) अपने नियंत्रण में प्रत्येक प्रणाली और नेटवर्क के संबंध में सुरक्षा की स्थिति की निगरानी

के लिए उत्तरदायी होंगे। सुरक्षा की कमजोरियों अथवा उल्लंघनों की सूचना संबंधित व्यावसायिक स्वामियों अथवा बुनियादी संरचना स्वामियों और सीआईएसओ को दी जाएगी जो फिर उक्त घटना की प्रतिक्रिया का समन्वय करेंगे।

च) प्रौद्योगिकी/परिचालन/प्रशासन/मानव संसाधन/कार्यात्मक दल अपनी टीम के एक उपयुक्त और अर्हताप्राप्त सदस्य को नामोद्दिष्ट करेंगे जो घटनाओं और सुरक्षा नियंत्रण

की प्रभावात्मकता की सूचना सीआईएसओ/ सूचना सुरक्षा दल/ सीआईओ को देने के लिए जिम्मेदार होगा।

छ) विधिक दल - विधिक दल आवश्यकता के अनुसार साइबर सुरक्षा पुलिस अधिकारियों, वकीलों और सरकारी एजेंसियों के साथ संबद्धता के लिए उत्तरदायी है। घटना से संबंधित आवश्यक ब्योरा सूचना सुरक्षा दल के द्वारा दिया जाएगा।

ज) प्रयोक्ता और सूचना स्वामी - प्रणाली प्रयोक्ता और डेटा स्वामी अपनी देखभाल अथवा नियंत्रण में स्थित प्रणालियों, डेटा, और अन्य सूचना स्रोतों के संबंध में नीतियों को लागू करने के लिए जिम्मेदार होंगे। वे किसी भी संदिग्ध साइबर सुरक्षा घटना की जानकारी सूचना सुरक्षा दल/ आईटी प्रमुख को देने के लिए भी उत्तरदायी हैं।

5.9.2 व्यवसाय स्वामियों के दायित्वः

व्यवसाय स्वामीः

क) जोखिम प्रबंध प्रक्रिया में सहभागिता करने और व्यवसाय प्रभाव निर्धारण करने के द्वारा अपने नियंत्रण के अंदर स्थित आस्तियों के मूल्य और वर्गीकरण को परिभाषित करने का प्राथमिक दायित्व वहन करेंगे।

ख) अनुप्रयोगों के अंदर निहित सूचना के अन्य पक्षकारों सहित वैयक्तिक प्रयोक्ताओँ और समूहों के लिए कर्तव्यों तक पहुँच और उनके पृथक्करण को प्राधिकृत करने के लिए उत्तरदायी होंगे।

ग) सुनिश्चित करेंगे कि आईएस नीति के अनुसार प्रवेश की व्यवस्था करने के लिए उनके अनुप्रयोगों हेतु प्रशासन की भूमिकाओं अथवा दलों की उपयुक्त पहुँच विद्यमान हो।

घ) अपनी व्यावसायिक इकाइयों के लिए यथाप्रयोज्य रूप में सूचना सुरक्षा नीतियों का कार्यान्वयन और अनुपालन सुनिश्चित करेंगे।

ङ) उन अन्य पक्ष भागीदारों और विक्रेताओं के जोखिम, डेटा सुरक्षा और प्रवेश के लिए, जिन्हें व्यवसाय की व्यवस्था का बाह्यस्रोतीकरण किया गया हो, प्राथमिक तौर पर उत्तरदायी होंगे।

च) परिभाषित आवृत्ति पर उन अन्य पक्षकारों के स्व-मूल्यांकन की समीक्षा करेंगे जिन्हें व्यवसाय की व्यवस्था का बाह्यस्रोतीकरण किया गया हो।

छ) अन्य पक्षकार प्रक्रियाओँ / स्थानों की सुरक्षा के निर्धारणों और संपरीक्षणों का संचालन करने के लिए उत्तरदायी होंगे।

ज) संस्था के सूचना सुरक्षा दल की सहमति के साथ अन्य पक्षकारों के लिए सूचना सुरक्षा संबंधी अपेक्षाओं को परिभाषित करेंगे।

5.10अनुरूपता

निम्नलिखित श्रेणी के प्रयोक्ता आईएस नीति का अनुपालन करने के लिए उत्तरदायी होंगे

क) वरिष्ठ प्रबंधक-वर्ग की प्राथमिक जिम्मेदारी, सूचना सुरक्षा के लिए एक सुस्पष्ट व्यवसाय सुयोजित कार्यक्रम विकसित करने, भूमिकाएँ और जिम्मेदारियाँ समनुदेशित करने, आईएस नीति का समर्थन करने तथा प्रायोजन और बजट उपलब्ध कराने की होगी जिससे यह सुनिश्चित किया जा सके कि उक्त कार्यक्रम का सफलतापूर्वक कार्यान्वयन किया गया है।

ख) सूचना के प्रयोक्ता की प्राथमिक जिम्मेदारी आईएस नीति के अंदर कार्य करते हुए सूचना सुरक्षा को कार्यान्वित करने की तथा सुरक्षा का उल्लंघन करने के लिए किसी

भी असाधारण, संदिग्ध अथवा पहचाने गये प्रयास की सूचना तत्परतापूर्वक देने की होगी।

5.11 प्रवर्तन

5.11.1 आंतरिक लेखा-परीक्षा

क) संस्था की आंतरिक लेखा-परीक्षा योजना के पास आईटी/प्रौद्योगिकी बुनियादी संरचना और अनुप्रयोगों को शामिल करते हुए एक अलग आईएस लेखा-परीक्षा योजना होगी। उक्त लेखा-परीक्षा योजना और रिपोर्टें बोर्ड की लेखा-परीक्षा समिति को प्रस्तुत की जाएँगी।

ख) कार्यान्वित किये गये अन्य पक्ष सुरक्षा नियंत्रणों की प्रभावात्मकता का मापन करने के लिए सुनियोजित और तदर्थ आधार पर महत्वपूर्ण डेटा को संभालनेवाले अन्य पक्षकारों/ विक्रेताओं के लिए लेखा-परीक्षा संचालित करेगी।

ग) सूचना की सुरक्षा से संबंधित अननुपालन के सभी उदाहरण सूचित किये जाएँगे तथा सुसंगत लाइन प्रबंध और सीआईएसओ के साथ इसके बारे में चर्चा की जाएगी।

5.11.2 सीआईएसओ

क) कमियों को ठीक करने में प्रबंधन और प्रयोक्ताओँ को सहायता प्रदान करेगा।

ख) अननुपालन संबंधी महत्वपूर्ण विषय समीक्षा और उपचारात्मक कार्रवाई के लिए आईएससी के ध्यान में लाएगा।

ग) कार्यान्वित किये गये नियंत्रणों की प्रभावात्मकता का मापन करने के लिए किसी विशिष्ट कार्य अथवा उत्पाद की एक निरंतर अथवा तदर्थ अन्य पक्ष समीक्षा/ निर्धारण प्रारंभ करेगा / करेगा तथा किसी असुरक्षितता पर विशेष बल देगा जिसे ठीक करने की आवश्यकता हो।

5.11.3 कार्यात्मक प्रौद्योगिकी टीमें -

क) अपने नियंत्रण में स्थित प्रत्येक प्रणाली और नेटवर्क के संबंध में सुरक्षा की स्थिति की नियमित निगरानी करने के लिए उत्तरदायी होंगी।

ख) सुरक्षा की कमजोरियों अथवा उल्लंघनों की सूचना संबंधित व्यावसायिक स्वामियों अथवा बुनियादी संरचना के स्वामियों और सीआईएसओ को देंगी, जो उक्त घटना की प्रतिक्रिया का प्रबंध करने के लिए उत्तरदायी होंगे।

ग) अंतिम स्थान प्रणाली (एण्ड पाइंट सिस्टम) और सर्वर सुरक्षा के संचालन के लिए उत्तरदायी होंगी।

5.12 जागरूकता

सभी हितधारकों को (कर्मचारियों, संविदागत स्टाफ आदि) को संस्थागत सूचना सुरक्षा नीतियों, प्रक्रियाओं और दिशानिर्देशों, आशंका के एक्सपोज़रों आदि से अवगत कराया जाएगा। उन्हें अपनी भूमिकाओं, जिम्मेदारियों के जानकार होने चाहिए तथा मानवीय त्रुटि के जोखिम को कम करने के लिए उनका पालन करना चाहिए।

5.12.1 सूचना सुरक्षा जागरूकताः-

क) समूचे संगठन में उपयुक्त हितधारकों और प्रयोक्ताओं को संप्रेषण के द्वारा आईएस नीति में ग्रहण किये गये रूप में व्यवसाय और सूचना सुरक्षा उद्देश्यों की समझ, परिचय और पहचान निर्मित करने के लिए प्रौद्योगिकी सहित पर्याप्त साधनों की व्यवस्था की जाएगी।

ख) प्रौद्योगिकीगत सुविधाओँ और वितरण माध्यमों का उपयोग करते समय सूचना प्रौद्योगिकी संबंधी करणीय (डूस) और अकरणीय (डोंट्स) के संबंध में विक्रेताओं और कर्मचारियों को शिक्षित करना।

ग) साइबर सुरक्षा की प्रवृत्तियों, प्रकारों अथवा नियंत्रणों के बारे में सामान्य और विशिष्ट जानकारी देना तथा उन्हें धोखाधड़ी निवारण के संबंध में अपनी जिम्मेदारियों से अवगत कराना।

5.13 प्रशिक्षण

संस्था यह सुनिश्चित करेगी कि सभी कार्मिक जिन्हें उत्तरदायित्व सौंपे गये हों, आवश्यक कार्य निष्पादित करने के लिए सक्षम हैं और उन्हें नियमित प्रशिक्षण दिया गया है।

5.13.1 सूचना सुरक्षा प्रशिक्षण के लक्ष्य

सभी कर्मचारी, और जहाँ लागू है वहाँ संविदागत स्टाफ, अन्य पक्ष सेवा प्रदाता और विक्रेता उनके कार्य के लिए संगत उपयुक्त सूचना सुरक्षा जागरूकता प्रशिक्षण अथवा आवधिक अद्यतन जानकारी प्राप्त करेंगेजिससे व्यवसाय के परिचालनों की सुरक्षा को सुनिश्चित किया जा सके।

5.14पहचान और प्रवेश प्रबंध

केवल प्राधिकृत `प्रयोक्ताओं' को व्यावसायिक अनुप्रयोगों/प्रणालियों/नेटवर्कों/संगणना के साधनों तक पहुँच की अनुमति देने के लिए पहचान के दायित्व और अधिप्रमाणन स्थापित करने के

द्वारा प्रभावी और सुसंगत प्रयोक्ता प्रबंध उपलब्ध कराने के लिए पहचान प्रबंध और प्रवेश नियंत्रण व्यवस्थाएँ स्थापित की जाएँगी।

5.14.1 सुरक्षा और प्रवेश नियंत्रण नीतियों और प्रक्रिया की स्थापना करना

क) प्रवेश नियंत्रण व्यवस्थाओं को चाहिए कि वे

I. प्रवेश को व्यावसायिक अनुप्रयोगों और प्रणालियों के मालिकों के द्वारा निर्धारित प्रवेश नीतियों के अनुरूप सीमित रखें।

II. व्यावसायिक अनुप्रयोग/प्रणाली/नेटवर्क/संगणना के साधन की क्षमताओं को, जिन तक पहुँचा जा सकता है (उदा. ऐसे मेनू/समूह उपलब्ध कराने के द्वारा जो केवल एक परिभाषित भूमिका का निर्वाह करने के लिए आवश्यक विशिष्ट क्षमताओं तकप्रवेश को संभव बनाते हैं), सीमित करें।

III. यदि आवश्यक हो और जब आवश्यक हो तब पासवर्डों का (उदा. स्मार्टकार्ड, बायोमेट्रिक्स अथवा टोकन जैसे सुदृढ़ अधिप्रमाणन का प्रयोग करने के द्वारा) संपूरण करें।

IV. विशेष प्रवेश विशेषाधिकारों की आवश्यकता को न्यूनतम बनाएँ (उदा. प्रयोक्ता आईडी जिनकी अतिरिक्त क्षमताएँ हों, जैसे प्रयोक्ता आईडी जिनका उपयोग भुगातनों को प्राधिकृत करने के लिए किया जा सकता है)।

V. दोनों व्यावसायिक प्रयोक्ताओं और कंप्यूटर स्टाफ के लिए प्रवेश का विशेषाधिकार प्रदान करने के लिए उपयुक्त प्राधिकारी से अनुमोदन/ व्यावसायिक अनुप्रयोग/ प्रणाली/ नेटवर्क/ संगणना साधन की अपेक्षा करें।

VI. सामान्य प्रयोक्ताओं एवं विशेषाधिकार प्राप्त प्रयोक्ताओं के प्रवेश को समाप्त करने के लिए एक प्रक्रिया लागू करें।

VII. आवधिक आधार पर समीक्षा करवाएँ।

VIII. व्यवसाय के मालिक, अनुमोदनकर्ताओं और उनके प्रत्यायोजित प्राधिकार के विवरण का अनुरक्षण किया जाएगा तथा उसका पुनःप्रमाणीकरण और अद्यतनीकरण आवधिक तौर पर किया जाएगा। प्राधिकृत करने की प्रक्रिया में आपातकालीन प्रवेश प्रदान करने की प्रक्रिया शामिल की जाएगी।

ख)विशेषाधिकार युक्त प्रवेश -

उच्चस्तरीय विशेषाधिकारों सहित, विशेषाधिकारों हेतु विशेष प्रवेश के लिए अतिरिक्त नियंत्रण लागू किये जाने चाहिए (उदा. यूनिक्स में `रूट' (मूल) अथवा विंडोस प्रणालियों में `एडमिनिस्ट्रेटर' (प्रबंधक)/शक्तिशाली उपयोगी सेवाएँ और विशेषाधिकार जिनका उपयोग भुगतानों को प्राधिकृत करने अथवा वित्तीय लेनदेन निष्पादित करने के लिए किया जा सकता है)

(ग) अधिप्रमाणन और पासवर्ड समक्रमण

सभी `प्रयोक्ताओँ'का अधिप्रमाणन उनके यूज़र आईडी और पासवर्डों का उपयोग करने के द्वारा न्यूनतम तौर पर, लक्ष्य प्रणालियों तक उनके प्रवेश पाने से पहले किया जाएगा जिससे संस्था की सूचना संबंधी आस्तियों तक अनधिकृत प्रवेश को रोका जा सके।

(घ) प्रावधानीकरण और प्रावधानीकरण का निरसन

अन्य पक्षकारों सहित सभी प्रयोक्ताओं के लिए रिपोजिटरी का अनुरक्षण किया जाना चाहिए।

5.14.2 प्रभावी प्रयोक्ता समूह प्रबंध -

क) आशोधन/ विलोपन - समूहः-

i) प्रवेश को समय पर अपेक्षित रूप में आशोधित किया जाएगा जब `प्रयोक्ता' आंतरिक रूप से स्थानांतरित होता है

ii) समय पर प्रवेश का प्रतिसंहरण किया जाएगा जब `प्रयोक्ता' बहिर्गमन करता है।

ख) पुनः प्रमाणीकरण -

i) अवांछित (स्ट्रे) / देखभाल-रहित (आर्फन) प्रयोक्ता खातों के अस्तित्व से बचने तथा यह सुनिश्चित करने के लिए कि प्रवेश के अधिकार जानने की आवश्यकता के आधार के सिद्धांत पर आधारित हैं, एक नियमित आधार पर संबंधित कार्यात्मक व्यावसायित मालिक द्वारा सभी प्रयोक्ता-आईडी और उनके प्रवेश अधिकार की समीक्षा की जाएगी।

ii) उक्त समीक्षा में यह सत्यापन भी शामिल होगा कि प्रयोक्ता के प्रवेश अधिकार और विशेषाधिकार अभी भी कार्य की आवश्यकताओं के अनुरूप हैं।

ग) जातीय (जिनेरिक) आईडी-

i) जातीय (जिनेरिक) प्रयोक्ता आईडी/सेवा आईडी से बचा जाएगा तथा जहाँ कोई विकल्प उपलब्ध न हो, वहाँ व्यवसाय/आस्ति के मालिक द्वारा इसे नियंत्रित किया जाएगा, प्राधिकृत किया जाएगा, जिससे प्रयोक्ता के दायित्व के साथ समझौता करने के लिए इसके दुरुपयोग से बचा जा सके।

ii) विशेषाधिकार जिनेरिक प्रयोक्ता-आईडी प्रयोक्ता को केवल उद्दिष्ट कार्यकलाप निष्पादित करने के लिए अनुमति देते हैं जिनके लिए प्रयोक्ता-आईडी निर्मित किये गये हों। ऐसे आईडी को व्यवसाय/आस्ति के मालिकों के द्वारा प्राधिकृत किया जाएगा।

घ) दूरस्थ प्रवेश-

i) संस्था के बुनियादी ढाँचे में दूरस्थ प्रवेश को, अविश्वस्त नेटवर्कों से संस्था के बुनियादी ढाँचे में अनधिकृत प्रवेश को रोकने के लिए अत्यधिक प्रतिबंधित किया जाएगा और नियंत्रित किया जाएगा।

ii) सार्वजनिक अथवा अन्य बाह्य नेटवर्कों के द्वारा संस्था की आईटी सुविधाओं में विशेषाधिकारयुक्त प्रवेश प्राप्त करने की अपेक्षा करनेवाले `प्रयोक्ता' इस प्रकार दो घटकों वाले अधिप्रमाणनों के द्वारा करेंगे।

5.15 परिवर्तन प्रबंध

व्यावसायिक अनुप्रयोगों, कंप्यूटर प्रणालियों और नेटवर्कों में परिवर्तन एक परिवर्तन प्रबंध प्रक्रिया का अनुसरण करेंगे जिसमें संबद्ध जोखिम, परिवर्तन प्राधिकरण, व्यवसाय निरंतरता और प्रभाव शामिल होंगे।

क. एक परिवर्तन प्रबंध प्रक्रिया स्थापित की जाएगी, जिसमें सभी प्रकार के परिवर्तन शामिल किये जाएँगे (उदा. अनुप्रयोग और साफ्टवेयर के कोटि-उन्नयन और आशोधन, व्यावसायिक सूचना में आशोधन, आपाती `जोड़' (फिक्सेज़) तथा कंप्यूटर प्रणालियों और नेटवर्कों में परिवर्तन)।

ख. परिवर्तन प्रबंध प्रक्रिया का प्रलेखीकरण किया जाएगा तथा इसमें यह सुनिश्चित करने के लिए परिवर्तनों का अनुमोदन करना और परीक्षण करना शामिल है किः

i) वे सही तौर पर और सुरक्षित रूप में किये गये हैं

ii) वे सुरक्षा नियंत्रणों के साथ कोई समझौता नहीं करेंगे

iii) कोई अनधिकृत परिवर्तन नहीं किये गये हैं तथा उत्पादन में केवल अनुमोदित परिवर्तन ही निर्मुक्त किये गये हैं

iv) वर्शन नियंत्रण का अनुरक्षण किया जाएगा ताकि यदि आवश्यक हो तो उसे वापस लिया जा सके।

v) अनधिकृत व्यक्ति को उत्पादन प्रणाली में परिवर्तन करने के लिए अनुमति दी जानी चाहिए।

5.16 परिवर्तन का कार्यान्वयन

क) परिवर्तन को निष्पादित करने के लिए कार्यान्वयन की योजना होगी जिसमें निम्नलिखित शामिल होंगे, परंतु जो केवल इन्हीं तक सीमित नहीं होगीः

i) कार्यान्वयन के चरण

ii) खराब होने के समय (डाउनटाइम) की आवश्यकताएँ/परियोजना की योजना

iii) परीक्षण योजना

iv) वापस लेने की योजना

ख) सफल कार्यान्वयन के लिए सभी परिवर्तनों की निगरानी की जाएगी तथा उनका प्रलेखीकरण किया जाएगा, वेः

i) कुशल और सक्षम व्यक्तियों द्वारा निष्पादित किये जाएँगे जो सही तौर पर और सुरक्षित रूप में परिवर्तन करने में सक्षम हैं। विकासकर्ता और निर्मोचन प्रबंधक / अभिनियोजन टीम प्रवेश को अलग किया जाना चाहिए।

ii) उपयुक्त व्यावसायिक मालिकों के द्वारा समाप्त किये जाएँगे।

iii) उनके वर्शन नियंत्रण और अभिग्रहण का अभिलेख होगा जिसका परिवर्तन किया गया तथा वह कब और किसके द्वारा किया गया।

iv) संबंधित व्यक्तिय़ों के साथ संचार का विवरण रखा जाएगा तथा यह पुष्टि करने के लिए परीक्षण निष्पादित किये जाएँगे कि केवल उद्दिष्ट परिवर्तन ही किये गये हैं।

v)सुनिश्चित करेंगे कि कंप्यूटर प्रणालियों और नेटवर्कों के साथ संबद्ध दस्तावेजों को अद्यतन किया गया है।

ग)डेटा अंतरण के दौरान / के बाद डेटा की अखंडता और गोपनीयता को सुनिश्चित करने के लिए पर्याप्त नियंत्रण रखा जाएगा तथा उसकी संपूर्णता का सत्यापन किया जाएगा।

घ) भावी समय के लिए, निर्मित किये गये डिजिटल अभिलेखों का पर्याप्त रूप से परिरक्षण किया जाना चाहिए तथा प्रौद्योगिकी में अनुवर्ती परिवर्तनों के बाद भी उन्हें पहुँच के योग्य और कार्यात्मक रखा जाना चाहिए।

5.17 विक्रेता/अन्य पक्ष जोखिम प्रबंध

अन्य पक्षकारों/विक्रेताओं की जब तक संस्थागत प्रणाली/डेटा में पहुँच रहती है/उनके द्वारा इन्हें संभाला जाता है, तब तक उस पूरी अवधि के दौरान सभी स्तरों पर सूचना की सुरक्षा की आवश्यकताओं का ध्यान रखा जाएगा।

5.17.1 बाह्य पक्ष प्रबंध

बाह्य पक्षकारों के साथ संबंधों की सुरक्षा का प्रबंध करने के लिए एक प्रक्रिया होगी। विक्रेता जोखिम प्रबंध की प्रक्रिया सूचना सूरक्षा कार्य को संबद्ध करेगी, तथा इसमें निम्नलिखित को शामिल किया जाएगा-

i. सुरक्षा टीम के साथ प्रत्येक बाहाय पक्षकार के लिए सुरक्षा व्यवस्थाओं (उदा. व्यवसाय की सुरक्षा की आवश्यकताओं और अन्य पक्षकार के अनुपालन की आवश्यकताओं के आधार पर) के विषय में सहमति होना।
ii. बाह्य पक्षकार/विक्रेताओं के साथ व्यवस्थाओं के संबंध में एक सुपरिभाषित सेवा स्तरीय करार (एसएलए) होगा जो सूचना सुरक्षा की आवश्यकताओं और नियंत्रणों, सेवा-स्तरों और एसएलए के उल्लंघनों की स्थिति में आपूर्तिकर्ताओं की देयता,

आईएस असुरक्षितताओँ के अन्यूनीकरण, आईएस घटनाओँ आदि को विनिर्दिष्ट करेगा। बाह्य पक्षकार सभी एसएलए अपेक्षाओँ का अनुपालन दर्शायेगा।

iii. प्रत्येक विक्रेता के लिए सुरक्षा व्यवस्थाओँ का विधिमान्यीकरण।

iv. किसी विक्रेता के साथ संबंध की समाप्ति को संभालना।

v. व्यवस्थाओँ की उप-संविदा करने के संबंध में समुचित सावधानी के पहलुओँ को सम्मिलित किया जाएगा।

vi. लेखा-परीक्षा/निरीक्षण का अधिकार।

तथापि, अंतिम दायित्व संस्था का होगा।

5.17.2 बाह्य पक्षकारों से संबंधित जोखिमों का समाधान करना

बाह्य पक्षकारों को संबद्ध करनेवाली व्यावसायिक प्रक्रियाओं से संस्था की सूचना और संबंधित सूचना प्रसंस्करण सुविधाओं के लिए जोखिमों की पहचान की जाएगी और निम्नलिखित परिदृश्यों में उपयुक्त नियंत्रण लागू किये जाएँगे।

5.17.2.1 नियुक्ति से पहले

i) बाह्य पक्षकार एक संबंध निर्धारण (कभी-कभी समुचित सावधानी समीक्षा के रूप में उल्लिखित) के अधीन होंगे जो निम्नलिखित को शामिल करेगाः

क) उपर्युक्त पक्षकार के साथ व्यवहार (उदा. प्रदाता का वृत्त, पिछला और वर्तमान व्यावसायिक व्यवस्था और विवाद संबंधी सूचना का ब्योरा)

ख) संविदा की अपेक्षाओँ में अप्रकटीकरण व्यवस्थाएँ, उप-संविदा करना, भूमिकाएँ और दायित्व, तथा समापन के खंड एवं संस्था, विधि प्रवर्तन एजेंसियों तथा आईआरडीएआई सहित विनियामक संस्थाओं द्वारा निरीक्षण/लेखा-परीक्षा का अधिकार शामिल होंगे।

ग) सूचना की सुरक्षा और सूचना की सुरक्षा के प्रति प्रतिबद्धता की मात्रा के संबंध में परिपक्वता का अन्य पक्षकार का प्रदर्शनयोग्य स्तर। यह इस क्षेत्र में उनकी परिपक्वता को शामिल करते हुए एक स्व-निर्धारित जाँच-सूची के माध्यम से है।

ii) जोखिम निर्धारण का संचालन संस्था की सूचना/सूचना प्रणालियों में अन्य पक्षकारों को प्रवेश प्रदान करने में संबद्ध जोखिमों का आकलन करने के लिए किया जाएगा।

iii) सुरक्षा नियंत्रणों की सूची को कार्यान्वित करने का निर्धारण नियुक्ति के प्रकार और सूचना की साझेदारी की आवश्यकता के स्वरूप के आधार पर किया जाएगा।

iv) डेटा की साझेदारी केवल `जानने की आवश्यकता' के आधार पर ही की जानी चाहिए।

5.17.2.2 नियुक्ति के दौरान

सुरक्षा निष्पादन और प्रवेश प्रबंधः

i. अन्य पक्षकारों के साथ गोपनीयता और अप्रकटीकरण करारों की समीक्षा आवधिक तौर पर तथा सेवा की शर्तों में जब भी परिवर्तन होता है तब की जाएगी।

ii. प्रवेश की अनुमति देने, प्रयोक्ता प्रवेश अधिकार की समीक्षा सहित अन्य पक्षकारों के लिए प्रवेश प्रबंध का निर्धारण आवधिक तौर पर की जाएगी तथा यथाप्रयोज्य रूप में इस संबंध में परिवर्तन किये जाएँगे।

iii. काल सेंटर परिचालन सम्मिलित करनेवाले अन्य पक्षकार के मामले में डेटा के प्रकटन को रोकने के लिए परिचालन प्रणाली को कठोर बनाया जाना चाहिए।

iv. बाह्य पक्षकार के आंतरिक नियंत्रणों की समीक्षाः

क) आंतरिक नियंत्रण की समीक्षा अपेक्षित करनेवाले बाह्य पक्षकारों की पहचान आवधिक आधार पर की जाएगी।

ख) समीक्षा के निष्कर्ष बाह्य पक्षकार को सूचित किये जाएँगे और सुधारात्मक कार्रवाई की निगरानी की जाएगी।

5.17.2.3 नियुक्ति का समापन अथवा नवीकरण

i) पक्षकारों के साथ संबंधों के समापन को सुरक्षा के साथ संभालने के लिए एक सुसंगत पद्धति स्थापित की जाएगी जिसमें निम्नलिखित शामिल किये जाएँगेः

क) समापन का प्रबंध करने के लिए जिम्मेदार व्यक्तियों को नामोद्दिष्ट करना

ख) संस्था की सूचना के प्रति भौतिक और तार्किक प्रवेश के अधिकारों का प्रतिसंहरण

ग) आस्तियों की वापसी, अंतरण अथवा सुरक्षित नाशन {उदा. `सहायक मीडिया संचयन' (बैक-अप मीडिया स्टोरेज)प्रलेखीकरण, हार्डवेयर और डेटा।}

घ) लाइसेंस करारों और बौद्धिक संपत्ति अधिकारों का कवरेज

ii) नवीकरण के मामले में, सुरक्षा संबंधी विचारों की समीक्षा नियुक्ति के परिदृश्य से पहले की स्थिति के अनुरूप करें।

5.18 व्यवसाय निरंतरता योजना

यह सुनिश्चित करने के लिए वैकल्पिक (आकस्मिकता) व्यवस्थाएँ स्थापित की जाएँगी कि उस स्थिति में जब बाह्य पक्षकार उपलब्ध नहीं है (उदा. संविदा के समापन के कारण या घोर संकट या बाह्य आपूर्तिकर्ता के साथ विवाद के कारण या इस वजह से कि प्रतियोगी (एन्ट्री) अपने परिचालन बंद कर देता है) तब संस्था की व्यावसायिक प्रक्रियाएँ जारी रह सकें। यह व्यवस्था एक जोखिम निर्धारण के परिणामों पर आधारित होगीः

वैकल्पिक, व्यावसायिक प्रक्रियाओँ के लिए सुरक्षित सुविधाओं की व्यवस्था जारी रहेगी।

i. संस्था एक विश्वस्त बाह्य पक्षकार, जैसे एक कानूनी प्रतिनिधि, न्यायवादी अथवा समकक्ष, का उपयोग करते हुए सूचना प्रणालियों के स्रोत कूट के लिए सहायता की समाप्ति / स्वामित्व प्रौद्योगिकियों (उदा. अनुप्रयोग स्रोत कूट और बीजलेखन (क्रिप्टोग्राफी) की कुंजियाँ) की समाप्ति के लिए निलंबसंपत्ति (एस्क्रो) का मूल्यांकन करेगी।

ii. एक बाह्यस्रोत प्रदाता के पास संचयन की गई सूचना की निरंतर उपलब्धता सुनिश्चित करने के लिए पुनःप्राप्ति की व्यवस्था।

iii. संस्था के व्यवसाय की निरंतरता के कार्यक्रम के साथ सुयोजन।

6. सूचना आस्ति प्रबंध

उद्देश्यः संस्थागत आस्तियों की पहचान करना, उपयुक्त संरक्षण और दायित्वों को परिभाषित करना। सूचना और सूचना प्रसंस्करण सुविधाओं के साथ संबद्ध आस्तियों की पहचान की जानी चाहिए तथा इन आस्तियों की एक सूची (इन्वेंटरी) बनाई जानी चाहिए और उसका अनुरक्षण किया जाना चाहिए। आस्तियों की उक्त इन्वेंटरी सही और अद्यतन होनी चाहिए।

पहचानी गई प्रत्येक आस्ति के लिए, आस्ति का स्वामित्व निर्दिष्ट किया जाना चाहिए और वर्गीकरण की पहचान की जानी चाहिए।

आस्ति के स्वामी को चाहिए कि वहः

क. आस्तियों की इन्वेंटरी को सुनिश्चित करे;

ख. सुनिश्चित करे कि आस्तियों का उपयुक्त रूप में वर्गीकरण और संरक्षण किया जाए;

ग. लागू प्रवेश नियंत्रण नीतियों को ध्यान में रखते हुए, महत्वपूर्ण आस्तियों के संबंध में प्रवेश प्रतिबंधों और वर्गीकरणों को परिभाषित करे और उनकी आवधिक तौर पर समीक्षा करे;

घ. जब आस्ति का विलोपन हो अथवा उसे नष्ट किया जाता है तब उचित रूप में संभालना सुनिश्चित करे।

सभी कर्मचारी और बाह्य पक्षकार प्रयोक्ता उनकी नियुक्ति, संविदा अथवा करार के समाप्त होने पर अपने कब्जे में स्थित सभी संस्थागत आस्तियाँ लौटाएँ।

समापन की प्रक्रिया को औपचारिक बनाया जाना चाहिए कि जिसमें संस्था द्वारा स्वामित्व-प्राप्त अथवा संस्था को सौंपी गई सभी पूर्व में जारी की गई भौतिक और इलेक्ट्रानिक आस्तियों की वापसी को शामिल किया जाए।

उन मामलों में जहाँ कोई कर्मचारी अथवा बाह्य पक्षकार प्रयोक्ता संस्था के उपस्कर खरीदता है अथवा अपने निजी उपस्कर का उपयोग करता है, वहाँ यह सुनिश्चित करने के लिए प्रक्रियाओं का पालन किया जाना चाहिए कि समस्त संगत सूचना का अंतरण संस्था को किया जाए और उपस्कर से सुरक्षित रूप में लुप्त किया जाए।

सूचना के लेबल लगाने के लिए प्रक्रियाओँ का उपयुक्त सेट विकसित किया जाना चाहिए और संस्था के द्वारा अपनाई गई सूचना के वर्गीकरण के अनुसार उसका कार्यान्वयन किया जाना चाहिए।

जब मीडिया की आवश्यकता न हो, तब औपचारिक प्रक्रियाओँ का उपयोग करते हुए मीडिया का निपटान सुरक्षित रूप से किया जाना चाहिए।

7.भौतिक और परिवेशगत सुरक्षा

उद्देश्यः संस्था की सूचना और सूचना प्रसंस्करण सुविधाओँ में अनधिकृत प्रवेश, क्षति और हस्तक्षेप को रोकना।

सुरक्षा परिमापों को परिभाषित किया जाना चाहिए तथा उन क्षेत्रों का संरक्षण करने के लिए इनका उपयोग किया जाना चाहिए जिनमें संवेदनशील अथवा महत्वपूर्ण सूचना, और सूचना प्रसंस्करण सुविधाएँ निहित हैं।

अनधिकृत भौतिक प्रवेश का निवारण करने के लिए जहाँ लागू हो, वहाँ भौतिक अवरोध बनाये जाने चाहिए।

निगरानी प्रणालियाँ विद्यमान होंगी तथा सभी प्रमुख क्षेत्रों को समाहित करने के लिए नियमित रूप से इनकी निगरानी की जाएगी।

यह सुनिश्चित करने के लिए कि केवल अधिकृत कार्मिकों को ही प्रवेश की अनुमति दी जाए, उपयुक्त प्रवेश नियंत्रणों के द्वारा सुरक्षित क्षेत्रों का संरक्षण किया जाना चाहिए।

सुरक्षित क्षेत्रों में प्रवेश के अधिकारों की नियमित रूप से समीक्षा की जाएगी और इन्हें अद्यतन किया जाएगा तथा जब आवश्यक हो तब इन्हें वापस लिया जाएगा।

अग्नि, बाढ़, भूकंप, विस्फोट, नागरिक अशांति जैसी विपदाओँ तथा अन्य प्रकार के प्राकृतिक अथवा मानव-निर्मित संकट का प्रबंध करने के लिए उपयुक्त नियंत्रण लागू किये जाएँगे।

नियंत्रणों की प्रभावात्मकता की जाँच करने के लिए आवधिक तौर पर नकली अभ्यास (माक ड्रिल्स) का संचालन किया जाएगा।
विद्युत भंग की स्थितियों से तथा सहायक साधनों में खराबी के कारण होनेवाले अन्य विघटनों से आईटी उपस्कर का संरक्षण किया जाना चाहिए।

प्रयोक्ताओं को यह सुनिश्चित करना चाहिए कि देखभाल से रहित उपस्कर का उपयुक्त संरक्षण किया जाना चाहिए।

कंप्यूटरों अथवा मोबाइल उपकरणों को प्रयोग न करने के समय अनधिकृत उपयोग से किसी `की लाक' अथवा उसके समकक्ष नियंत्रण, उदा. पासवर्ड के जरिये प्रवेश के द्वारा सुरक्षित रखा जाएगा।

कागज-पत्रों और हटाने योग्य स्टोरेज मीडिया के लिए एक स्वच्छ डेस्क नीति और सूचना प्रसंस्करण सुविधाओँ के लिए एक स्वच्छ स्क्रीन नीति अपनाई जानी चाहिए।

8. मानव संसाधन सुरक्षा

उद्देश्यः यह सुनिश्चित करना कि कर्मचारी और ठेकेदार अपने उत्तरदायित्वों को समझें और उन भूमिकाओं के लिए वे उपयुक्त हों जिनके लिए उनके संबंध में विचार किया गया है।

नियोजन के लिए सभी उम्मीदवारों के संबंध में पृष्ठभूमि के सत्यापन की जाँच संबंधित कानूनों, विनियमों और आचार-शास्त्र के अनुसार संचालित की जानी चाहिए तथा वह

व्यावसायिक आवश्यकताओं, निर्धारित की जानेवाली सूचना के वर्गीकरण और ज्ञात जोखिमों के विषय में आनुपातिक रूप में होनी चाहिए।

सूचना सुरक्षा संबंधी भूमिकाओं और दायित्वों की जानकारी नियोजन-पूर्व प्रक्रिया के दौरान नौकरी के उम्मीदवारों को दी जानी चाहिए।

गोपनीयता, डेटा संरक्षण, नीतिशास्त्र, संस्था के उपस्कर और सुविधाओं के उपयुक्त उपयोग एवं संस्था के द्वारा प्रत्याशित प्रतिष्ठित व्यवहारों के संबंध में कर्मचारियों अथवा ठेकेदारों के सूचना सुरक्षा संबंधी उत्तरदायित्व बताने के लिए एक आचरण-संहिता लागू की जा सकती है।

जागरूकता, शिक्षा और प्रशिक्षण के कार्यकलाप व्यक्ति की भूमिकाओं, उत्तरदायित्वों और कुशलताओं के लिए उपयुक्त और संगत होने चाहिए।
जिन कर्मचारियों ने सूचना सुरक्षा का उल्लंघन किया हो, उनके विरुद्ध कार्रवाई करने के लिए एक औपचारिक और संसूचित अनुशासन की प्रक्रिया लागू की जानी चाहिए।

9. प्रणाली अधिग्रहण, विकास और अनुरक्षण

उद्देश्यः यह सुनिश्चित करना कि सूचना सुरक्षा समूचे प्रणाली विकास जीवनचक्र में सूचना प्रणालियों का एक अभिन्न अंग हो।

सूचना सुरक्षा संबंधी आवश्यकताओँ और संबद्ध प्रक्रियाओँ की पहचान औऱ प्रबंध का समन्वय सूचना प्रणालियों की परियोजनाओँ के प्रारंभिक स्तरों में किया जाना चाहिए। सूचना सुरक्षा संबंधी आवश्यकताओं का समय पर, उदा. अभिकल्पन के स्तर पर, ध्यान रखना अधिक प्रभावी और किफायती समाधानों के लिए मार्ग प्रशस्त कर सकता है।

उत्पादों (साफ्टवेयर और समाधान) को स्वीकार करने के लिए मानदंड परिभाषित किये जाने नसुरक्षा संबंधी आवश्यकताएँ पूरी की गई हैं। अधिग्रहण से पहले उत्पादों का मूल्यांकन इन मानदंडों के आधार पर किया जाना चाहिए।

10. सूचना सुरक्षा जोखिम प्रबंध

उद्देश्यः उन व्यक्तियों को समर्थ बनाना जो मुख्य सूचना जोखिमों की पहचान करने और उन जोखिमों को स्वीकार्य सीमाओँ के अंदर रखने के लिए आवश्यक नियंत्रणों का निर्धारण करने हेतु लक्ष्य परिवेशों के लिए उत्तरदायी हैं।

नीतिगत प्रक्रिया और दिशानिर्देशः संस्था के पास एक आवधिक आधार पर लक्ष्य परिवेशों (उदा. महत्वपूर्ण व्यावसायिक परिवेश, व्यावसायिक प्रक्रियाएँ, व्यावसायिक अनुप्रयोग, कंप्यूटर प्रणालियाँ और नेटवर्क) के लिए सूचना सुरक्षा जोखिम निर्धारण करने हेतु एक जोखिम प्रबंध कार्यक्रम होना चाहिए।

10.1 सूचना सुरक्षा जोखिम निर्धारण का प्रबंध करना

10.1.1 सूचना जोखिम निर्धारणों का निष्पादन करने के लिए औपचारिक, प्रलेखीकृत मानक/ प्रक्रियाएँ होंगी, जो समूची संस्था में लागू होंगी। मानक प्रक्रियाएँ निम्नलिखित को कवर करेंगीः

क. सूचना सुरक्षा जोखिम निर्धारण की आवश्यकता

ख. लक्ष्य परिवेश के प्रकार जिनका निर्धारण सूचना जोखिमों के लिए किया जाएगा, उदा. आईटी अनुप्रयोग, हार्डवेयर और साफ्टवेयर विक्रेका, आदि।

ग. परिस्थितियाँ जिनमें सूचना निर्धारण निष्पादित किये जाएँगे

घ. व्यक्ति जिन्हें संबद्ध करने की आवश्यकता है और उनकी विशिष्ट जिम्मेदारियाँ - व्यवसाय के स्वामी, जोखिम निर्धारण में विशेषज्ञ, आईटी, आदि।

ङ. सूचना जोखिम निर्धारणों के परिणामों का प्रबंध औऱ न्यूनीकरण करने की पद्धति

10.1.2 समूची संस्था में संचालित सूचना सुरक्षा जोखिम निर्धारणों के परिणामः

क. व्यवसाय के स्वामियों और वरिष्ठ प्रबंधन अथवा समकक्ष को सूचित किये जाएँगे

ख. सूचना सुरक्षा कार्यक्रम में सहायता के लिए प्रयुक्त किये जाएँगे

ग. अधिक व्यापक जोखिम प्रबंध कार्यकलापों के साथ समन्वित किये जाएँगे

घ. सूचना सुरक्षा जोखिम प्रबंध स्थापित करेंगे

ङ. सूचना जोखिम प्रबंध (आईआरएम) के विस्तार को परिभाषित करेंगे

च. जोखिम निर्धारण के प्रति प्रणालीगत दृष्टिकोण को परिभाषित करेंगे

छ. आईआरएम के विस्तार के अंदर आस्तियों के प्रति जोखिम की पहचान करेंगे

ज. जोखिमों का निर्धारण, जोखिमों कीअभिक्रिया/उपचारात्मक उपायों के लिए विकल्पों की पहचान और उनका मूल्यांकन किया जाएगा

झ. जोखिम की अभिक्रिया के लिए नियंत्रण लक्ष्यों और नियंत्रणों का चयन करेंगे तथा सूचना जोखिम प्रबंध का कार्यान्वयन और परिचालन करेंगे

ञ. जोखिम अभिक्रिया योजना बनाएँगे और उसे कार्यान्वित करेंगे

ट. नियंत्रण के उद्देश्यों को पूरा करने के लिए चयनित नियंत्रणों को कार्यान्वित करेंगे।

ठ. आईआरएम संबंधी परिचालनों और संसाधनों का प्रबंध करेंगे।

ड. सुरक्षा संबंधी घटनाओँ की पहचान और प्रतिक्रिया करने के लिए प्रक्रियाओँ और अन्य नियंत्रणों का कार्यान्वयन करेंगे

ढ. सूचना जोखिम प्रबंध की निगरानी और समीक्षा करेंगे।

10.1.3 निम्नलिखित हेतु निगरानी प्रक्रियाओँ और अन्य नियंत्रणों का कार्यान्वयनः

क. प्रसंस्करण के परिणामों में त्रुटियों की पहचान तुरंत करना

ख. विफल और सफल सुरक्षा उल्लंघनों और घटनाओँ की तुरंत पहचान करना

ग. यह निर्धारण करने में प्रबंधन को समर्थ बनाना कि क्या लोगों को प्रत्यायोजित अथवा सूचना प्रौद्योगिकी द्वारा कार्यान्वित सुरक्षा कार्यकलाप प्रत्याशित रूप में निष्पादन कर रहे हैं

घ. व्यवसाय की प्राथमिकताओँ को प्रतिबिंबित करते हुए, सुरक्षा के उल्लंघन का समाधान करने के लिए की गई कार्रवाइयों का निर्धारण करना

ङ. आईआरएम कार्य योजना की प्रभावात्मकता की नियमित समीक्षाएँ करना

च. अवशिष्ट जोखिम और स्वीकार्य जोखिम के स्तर की समीक्षा करना

छ. सूचना जोखिम प्रबंध को बनाये रखना और उसमें सुधार लाना

ज. आईआरएम कार्य योजना में अभिनिर्धारित सुधारों को कार्यान्वित करना

झ. उपयुक्त सुधारात्मक और निवारक कार्रवाइयाँ करना

ञ. परिणाम और कार्रवाइयाँ संबंधित टीमों को सूचित करना तथा सुधार योजनाओँ के संबंध में सीआईएसओ के साथ परामर्श करना

ट. सुनिश्चित करना कि सुधार अपने उद्दिष्ट लक्ष्य को प्राप्त करेंगे

10.2 सूचना सुरक्षा नीति - स्वीकार्य उपयोग

सूचना, उसके रूप का विचार किये बिना, संस्था के लिए एक मूल्यवान आस्ति है। सूचना सुरक्षा नीति का उद्देश्य सूचना की गोपनीयता, संपूर्णता और उपलब्धता को सुनिश्चित करना है। सभी कर्मचारियों में सुरक्षा संस्कृति कायम करना जो संस्था की सूचना सुरक्षा नीति और सूचना सुरक्षा रणनीति का समर्थन करे। सूचना सुरक्षा नीति अंतिम उपयोगकर्ताओँ के लिए स्वीकार्य उपयोग से संबंधित तत्वों को समाविष्ट करेगी जो समूची संस्था में एक सुरक्षित परिवेश का निर्माण करने में सहायता करेंगे।

स्वीकार्य उपयोग नीति में निम्नलिखित शामिल होंगेः

- सूचना का वर्गीकरण और नाम रखना (लेबलिंग)
- पासवर्ड प्रबंध
- अंतिम बिन्दु (डेस्कटाप/लैपटाप और मोबाइल साधन)
    - असुरक्षित सेवाओँ और संसाधनों को अशक्त करते हुए मानक विन्यास (कान्फिगरेशन), वाइरस/मालवेयर संरक्षण
    - अनधिकृत/अ-मानक साफ्टवेयर के संस्थापन को रोकने के लिए नियंत्रण
- तर्कसंगत प्रवेश
- सुनिश्चित (क्लियर) डेस्क
- इंटरनेट प्रवेश नीति
- ई-मेल नीति
- बाह्य/सुवाह्य (पोर्टबल) भंडारण साधनों का उपयोग
- तत्काल संदेश-प्रेषण और सोशल मीडिया
- दूरस्थ पहुँच
- बेतार पहुँच

10.3 व्यवसाय निरंतरता और संकट समुत्थान ढाँचा

10.3.1 व्यवसाय निरंतरता नीति और प्रबंध

क. संस्था के पास एक व्यवसाय निरंतरता नीति (बीसीपी) होगी, जो स्पष्ट रूप से अभिनिर्धारित दायित्वों से युक्त होगी।

ख. बीसीपी को संस्था के जोखिम प्रबंध का एक मुख्य पहलू होना चाहिए।

ग. उक्त नीति संस्था के विभिन्न स्तरों पर व्यवसाय निरंतरता के साथ संबद्ध अथवा उसके लिए जिम्मेदार सभी व्यक्तियों को सूचित की जाएगी।

घ. आवधिक तौर पर अथवा कोई महत्वपूर्ण परिवर्तन होने की स्थिति में उक्त नीति की समीक्षा की जाएगी।

ङ. व्यवसाय निरंतरता के प्रभावी कार्यान्वयन और परिचालन के लिए आवश्यक संसाधन, जैसे कार्य क्षेत्र और श्रम शक्ति आदि, उपलब्ध कराये जाने चाहिए।

10.3.2 व्यवसाय निरंतरता की जागरूकता

क. उक्त बीसी नीति कर्मचारियों को सूचित की जानी चाहिए और उनके पास उपलब्ध होनी चाहिए।

ख. संबंधित कर्मचारियों के लिए स्टाफ प्रशिक्षण कार्यक्रम

10.3.3 उक्त बीसीपी में निम्नलिखित निहित होने चाहिएः

क. व्यवसाय प्रभाव विश्लेषण

ख. व्यवसाय निरंतरता रणनीति/योजना

ग. आपाती प्रतिक्रिया योजना

घ. बीसीपी परीक्षण रिपोर्टें

10.3.4 महत्वपूर्ण व्यवसाय प्रक्रियाओं, उनका समर्थन करने के लिए आवश्यक संसाधनों तथा अनुपलब्धता की स्थिति में समय पर प्रभाव के मापन की पहचान करने के लिए व्यवसाय के प्रभाव का विश्लेषण संचालित किया जाना चाहिए।

10.3.5 मुख्य व्यवसाय प्रक्रियाओं में किसी भी विघटन के प्रभाव का निर्धारण करने के लिए एक सुपरिभाषित पद्धति होगी।

10.3.6 संस्था स्वीकार्य समय के अंदर अभिनिर्धारित महत्वपूर्ण गतिविधियों के समुत्थान के लिए उपयुक्त व्यवसाय निरंतरता व्यवस्थाओं की पहचान करेगी।

10.3.7 डीआर में आवश्यक समर्थक प्रणालियों अथवा प्रक्रियाओं (गैर-महत्वपूर्ण) की पहचान

की जानी चाहिए तथा स्वीकार्य सहिष्णुता स्तरों के साथ समुत्थान की योजना बनाई जानी चाहिए।

10.3.8 संस्था आपाती प्रतिक्रिया संरचना विकसित करेगी जो घटना का प्रबंध करेगी और उसके महत्वपूर्ण कार्यकलापों की निरंतरता सुनिश्चित करेगी।

10.3.9 संस्था अपनी व्यवसाय निरंतरता आयोजना की चालू प्रभावात्मकता को आवधिक परीक्षण के द्वारा विधिमान्य करेगी तथा अपेक्षित कार्रवाइयों सहित प्रयोग, परिणाम और शिक्षा की रिपोर्ट तैयार करेगी।

10.3.10 प्रबंधन **संस्था की व्यवसाय निरंतरता की तैयारी की समीक्षा सुनियोजित** अंतरालों

पर अथवा जब महत्वपूर्ण परिवर्तन घटित होते हैं तब **करेगा**।

11. डेटा सुरक्षा

उद्देश्यः संस्थाएँ स्वीकार करेंगी कि उनकी डेटा सुरक्षा का कुशल प्रबंध उनके मुख्य कार्यों को समर्थन देने, उनके सांविधिक और विनियामक दायित्वों का अनुपालन करने तथा प्रभावी समग्र प्रबंधन में अंशदान देने के लिए आवश्यक है।

विस्तारः संस्थाओँ के लिए विभिन्न रूपों में रखे गये समस्त डेटा की गोपनीयता, संपूर्णता, उपलब्धता और सुसंगति को सुनिश्चित करने के लिए क्रियाविधियों को परिभाषित और क्रियान्वित करने की आवश्यकता है। ये दिशानिर्देश संस्था के सभी स्थायी और अस्थायी कर्मचारियों और परामर्शदाताओँ (सामूहिक तौर पर "कर्मचारियों"), अन्य पक्ष विक्रेताओँ तथा व्यवसाय वितरकों, जिनकी पहुँच संस्था के डेटा तक हो, द्वारा निर्मित अथवा अनुरक्षित समस्त सूचना/अभिलेखों/डेटा के लिए लागू हैं, जहाँ भी इस डेटा के अभिलेख हों तथा उनके निर्दिष्ट कर्तव्यों और कार्यों का निर्वाह करने के दौरान वे किसी भी रूप में हों।

11.1 डेटा सुरक्षा नीति की योजना

उभरते हुए उपभोक्तीकरण (कन्स्यूमराइजेशन), क्लाउड कंप्यूटिंग की वृद्धि, व्यवसाय निरंतरता के बढ़े हुए महत्व, साइबर अपराध के संवर्धित सातत्य तथा आंतरिक आशंकाओं के प्रति बढ़ी हुई अरक्षितता जैसी हाल की महाप्रवृत्तियों (मेगाट्रेंड्स) का समग्र अवलोकन दर्शाता है कि डेटा संरक्षण संस्थाओं के लिए एक महत्वपूर्ण चुनौती के रूप में लगातार बना रहेगा जो बढ़ते हुए डेटा जोखिम के रूप में परिणत होगा।

डेटा के रूप में सूचना का एक प्राकृतिक जीवन-चक्र है जो उसके निर्माण और उत्पादन से लेकर भंडारण, प्रसंस्करण, उपयोग तथा अंतरण के माध्यम से उसके अंतिम नाशन अथवा अपक्षय तक है। डेटा आस्तियों का मूल्य, और उसके लिए जोखिम उनके जीवन-काल के दौरान भिन्न हो सकते हैं, परंतु डेटा सुरक्षा सभी स्तरों पर कुछ सीमा तक महत्वपूर्ण रहती है।

	स्रोत पर डेटा	
डेटा नाशन		संचलन में डेटा
विराम पर डेटा		प्रयोग में डेटा

अतः डेटा जीवन-चक्र के प्रत्येक स्तर पर, संस्थाएँ गोपनीयता, संपूर्णता और उपलब्धता के प्रति समुचित ध्यान सुनिश्चित करेंगी। नीचे उल्लिखित रूप में निम्नलिखित डेटा सुरक्षा नियंत्रणों का ध्यान रखा जाएगाः

- प्रणाली में प्रविष्ट डेटा की सुसंगति और सहीपन का सत्यापन जहाँ भी लागू है वहाँ निर्माता (मेकर)- जाँचकर्ता (चेकर) प्रक्रिया के द्वारा किया जाना चाहिए। यह सुनिश्चित करने के लिए एक प्रक्रिया होनी चाहिए कि परस्पर-विरोधी भूमिकाओं के लिए ऐसे मेकर-चेकर कार्यों के अनुसरण में कर्तव्यों का पृथक्करण किया जाए तथा एक ही प्रयोक्ता दोनों कार्य निष्पादित नहीं कर सकता।
- महत्वपूर्ण डेटा का अनुवर्ती लेखा-परीक्षण (आडिट ट्रेल) बनाये रखा जाएगा। साक्ष्य के परिरक्षण सहित, प्राप्त सूचना की संपूर्णता को सुनिश्चित करने के लिए लेखा-परीक्षणों को सुरक्षित रखा जाना चाहिए।लेखा-परीक्षणों का प्रतिधारण व्यवसाय, विनियामक और कानूनी अपेक्षाओं के अनुरूप होना चाहिए।
- यह सुनिश्चित करने के लिए प्रवेश `जानने की आवश्यकता' अथवा `न्यूनतम विशेषाधिकार' के आधार पर दिया जाना चाहिए कि आवश्यक कार्मिकों (कर्मचारियों) को आवश्यक प्रणाली में प्रवेश मिले तथा इस प्रवेश की आवधिक तौर पर समीक्षा की जानी चाहिए।
- कागज पर उत्पन्न / निर्मित किये गये डेटा के लिए प्रयोक्ता को यह सुनिश्चित करना चाहिए कि वह डेटा वर्गीकरण नीति का पालन करे, कार्यालय में उसे एक सुरक्षित स्थान पर रखा जाए तथा डेटा के सीआईए का अनुरक्षण किया जाए।
- संस्थाओं में सभी नये कर्मचारियों के संबंध में कार्य अनुप्रयोग सूचना का सत्यापन करने के लिए एक प्रक्रिया होनी चाहिए। संस्थाओं को यह सत्यापन करना चाहिए कि ठेकेदार भी इसी प्रकार की अनुवीक्षण (स्क्रीनिंग) प्रक्रियाओं के अधीन हों।
- विशिष्ट संस्थागत डेटा अभिलेखों के संरक्षण पर विचार करते समय, संस्थाओं की वर्गीकरण योजना के आधार पर उनके संबंधित तदनुरूपी वर्गीकरण पर विचार किया जाना चाहिए। एक बार डेटा का वर्गीकरण किये जाने पर, प्रयोक्ताओं का यह दायित्व होगा कि वे यह सुनिश्चित करें कि नीति के अनुसार पर्याप्त नियंत्रणों का पालन किया जाएगा तथा महत्वपूर्ण डेटा भंडारण स्थानों की सूची (इन्वेंटरी) का अभिनिर्धारण किया जाएगा और उसका प्रलेखीकरण किया जाएगा।
- व्यवसाय के लिए संवेदनशील / महत्वपूर्ण डेटा को सुरक्षित रखने के लिए, महत्वपूर्ण डेटा का अभिनिर्धारण करने के लिए एक व्यवस्था व्यवसाय पर उसके प्रभाव के आधार पर परिभाषित की जाएगी।

- महत्वपूर्ण डेटा को सँभालने के बारे में प्रयोक्ताओँ को नियमित जागरूकता कार्यक्रमों के द्वारा, डेटा के वर्गीकरण स्तर नियमित रूप से प्रदान किये जाएँगे।
- प्रयोक्ताओँ से गोपनीयता का वचन-पत्र प्राप्त किया जाएगा।
- लैपटाप अथवा अन्य साधनों की हानि होने की स्थिति में डेटा के प्रकटीकरण से बचने के लिए लैपटापों और अन्य मोबाइल साधनों पर स्थित महत्वपूर्ण डेटा का संरक्षण किया जाएगा।
- मीडिया का सुरक्षित भंडारण होना चाहिए। नियंत्रणों में भौतिक और परिवेशगत नियंत्रण, जैसे अग्नि और बाढ़ से संरक्षण, भौतिक तालों, की-पैड, पासवर्डों, बायोमैट्रिक्स आदि साधनों तथा लेबलिंग, और लागिंग से युक्त प्रवेश के द्वारा प्रवेश को सीमित करना शामिल हो सकते है।
- मार्गस्थ और भंडारण में स्थित महत्वपूर्ण और संवेदनशील डेटा/सूचना तक पहुँच को नियंत्रित करने के लिए क्रिप्टोग्राफिक/पासवर्ड प्रबंध तकनीकों का प्रयोग करने की आवश्यकता है।
- यदि संवेदनशील डेटा बाह्यस्रोतीकरण (आउटसोर्सिंग) सेवा प्रदाता को, व्यवसाय के प्रयोजन के लिए अन्य पक्षकार को भेजने की आवश्यकता हो, तो वह सूचना/ व्यवसाय के स्वामी के द्वारा अनुमोदित किया जाएगा तथा यह सुनिश्चित करने के लिए नियंत्रण अभिकल्पित किये जाएँगे कि अन्य पक्षकार के द्वारा डेटा का दुरुपयोग नहीं किया जाएगा। (एनडीए, अधिकार संरक्षित ई-मेल आदि)
- डेटा को अभिलेखागार में रखते समय डेटा की संपूर्णता और गोपनीयता को अनुरक्षित करने के लिए पर्याप्त नियंत्रण बनाये रखे जाएँगे। जब डेटा को भंडारण में अभिलेखागार के अधीन रखा जाएगा, तब डेटा के संबंध में उचित प्रवेश नियंत्रण होने चाहिए।

निपटान व्यवस्थाओं को डेटा का प्रभावी नाशन सुनिश्चित करना चाहिए। ऐसी व्यवस्थाओं में शामिल हैं, डिजिटल फाइल श्रेडिंग, चुंबकीय विक्षेत्रण (डीगाउसिंग) (अर्थात् रिकार्ड किये गये डेटा को मिटाने के लिए मैग्नेटिक मीडिया को मैग्नेटरहित करने की प्रक्रिया) तथा भंडारण मीडिया का भौतिक नाशन (उदा. चूर्णन, भस्मीकरण अथवा श्रेडिंग)। नष्ट करने की एक पद्धति के रूप में रीफार्मेटिग का भी प्रयोग किया जा सकता है यदि यह गारंटी दी जा सकती है कि उक्त प्रक्रिया को नहीं उलट दिया जा सकता। किसी डिजिटल अभिलेख के संपूर्ण नाशन को सुनिश्चित करने के लिए, विद्यमान सभी प्रतियों का पता लगाया जाना चाहिए और उन्हें नष्ट किया जाना चाहिए। इसमें प्रणाली बैक-अपों और परोक्ष भंडारण में निहित प्रतियों को हटाना और नष्ट करना शामिल है।

12. अनुप्रयोग सुरक्षा

उद्देश्यः यह सुनिश्चित करना कि सूचना सुरक्षा, समूचे जीवन-चक्र में सूचना प्रणालियों का एक अभिन्न अंग है तथा इसमें सूचना प्रणालियों के लिए आवश्यकताएँ भी शामिल हैं, जो सार्वजनिक नेटवर्कों पर सेवाएँ उपलब्ध कराती हैं।

महत्वपूर्ण अनुप्रयोग नियंत्रण और जोखिम न्यूनीकरण उपाय निम्नलिखित हैं जिनके संबंध में संस्था के द्वारा कार्यान्वयन के लिए विचार किया जाना चाहिएः

12.1 प्रत्येक अनुप्रयोग का एक स्वामी होना चाहिएः

अनुप्रयोग/व्यवसाय स्वामियों की कुछ भूमिकाओं में निम्नलिखित शामिल होंगेः

क) अनुप्रयोग में किये जानेवाले किन्हीं परिवर्तनों को प्राथमिकता से युक्त बनाना और उन परिवर्तनों को प्राधिकृत करना।

ख) किसी अनुप्रयोग से संबंधित डेटा के लिए डेटा का वर्गीकरण/अवर्गीकरण और अभिलेखागार में रखने/मिटाने (पर्जिंग) की क्रियाविधियों के विषय में संबंधित नीतियों/ विनियामक/सांविधिक अपेक्षाओं के अनुसार व्यवसाय स्वामियों की सहमति से विचार करना।

ग) यह सुनिश्चित करना कि अनुप्रयोग के अभिकल्पन, विकास, परीक्षण और परिवर्तन की प्रक्रिया में सक्रिय संबद्धता के द्वारा अनुप्रयोग में पर्याप्त नियंत्रण निर्मित किये जाएँ।

घ) यह सुनिश्चित करना कि अनुप्रयोग में किसी भी परिवर्तन के लिए परिवर्तन प्रबंध प्रक्रिया का अनुसरण किया जाए।

ङ) यह सुनिश्चित करना कि अनुप्रयोग प्रयोक्ताओं की व्यावसायिक/कार्यात्मक आवश्यकताएँ पूरी करता है।

च) यह सुनिश्चित करना कि अनुप्रयोग की सुरक्षा की समीक्षा की गई है।

छ) अधिगृहीत / विकसित किये जानेवाले किन्हीं नये अनुप्रयोगों अथवा निकाल दिये जानेवाले किन्हीं पुराने अनुप्रयोगों के संबंध में निर्णय लेना।

ज) किसी अनुप्रयोग की खरीद के संबंध में सूचना सुरक्षा टीम को सूचित करना तथा अनुप्रयोग का निर्धारण सुरक्षा नीति की अपेक्षाओं के आधार पर करना।

झ) यह सुनिश्चित करना कि खरीदे जानेवाले/ विकसित किये जानेवाले नये अनुप्रयोगों के संबंध में सूचना सुरक्षा नीति का पालन किया जाए।

ञ) यह सुनिश्चित करना कि अनुप्रयोगों के लिए अपेक्षित रूप में लागों और अनुवर्ती लेखा-परीक्षाओं (आडिट ट्रेल्स) को समर्थ बनाया जाए और उनकी निगरानी की जाए। महत्वपूर्णता के आधार पर लाग कम से कम कौन-कब-क्या-कहाँ के मानदंडों को पूरा करें।

ट) सभी इंटरनेट पोर्टल अनुप्रयोगों के लिए अंतिम लाग-इन विवरण अनुरक्षित किये जाएँ।

ठ) प्रवेश और भूमिकाओँ की समीक्षा आवधिक तौर पर संचालित करना सुनिश्चित किया जाए।

12.2 सूचना सुरक्षा अपेक्षाओँ का विश्लेषण और विशिष्टीकरण

क) सूचना सुरक्षा संबंधी अपेक्षाएँ वर्तमान सूचना प्रणालियों में नई सूचना प्रणालियों अथवा वृद्धियों के विकास के लिए अपेक्षाओँ में शामिल की गई हैं।

ख) व्यावसायिक कार्यात्मकताओं के अलावा, प्रणाली प्रवेश नियंत्रण, अधिप्रमाणन, लेनदेन प्राधिकरण, डेटा की संपूर्णता, प्रणाली कार्यकलाप लागिंग, अनुवर्ती लेखा-परीक्षा (आडिट ट्रेल), सुरक्षा घटना की खोज और अपवर्जन संभलाई आदि से संबंधित सुरक्षा अपेक्षाएँ प्रणाली के विकास/अधिग्रहण के प्रारंभिक चरणों में स्पष्ट रूप से विनिर्दिष्ट करने की आवश्यकता है।

ग) परिवर्तन के अनुरोध और की गई तदनुरूपी कार्रवाई के बीच उचित संबद्धता होनी चाहिए।

घ) किसी अनुप्रयोग प्रणाली/ डेटा में किसी भी परिवर्तन के लिए वास्तविक व्यावसायिक आवश्यकता के द्वारा तर्कसंगत सिद्ध किये जाने की आवश्यकता है और अनुमोदन प्रलेखीकरण के द्वारा समर्थित होने चाहिए तथा एक सुदृढ़ प्रबंध प्रक्रिया के अधीन किये जाने चाहिए।

12.3 परिचालन प्लेटफार्म परिवर्तनो के बाद अनुप्रयोगों की तकनीकी समीक्षा

जब परिचालन प्लेटफार्म परिवर्तित किये जाते है, तब व्यावसाय के महत्वपूर्ण अनुप्रयोगों की समीक्षा की जानी चाहिए और यह सुनिश्चित करने के लिए उनकी जाँच की जानी चाहिए कि संस्थागत परिचालनों अथवा सुरक्षा पर कोई प्रतिकूल प्रभाव न हो।

12.4 सुरक्षा प्रणाली इंजीनियरिंग सिद्धांत

क. सुरक्षा प्रणालियों के प्रबंध (इंजीनियरिंग) के लिए सिद्धांत किसी भी सूचना प्रणाली कार्यान्वयन प्रयासों के संबंध में स्थापित, प्रलेखीकृत, अनुरक्षित और लागू किये जाएँगे।

ख. अनुप्रयोग के प्रबंध के लिए प्रलेखीकृत मानक/क्रियाविधियाँ होनी चाहिए तथा उन्हें आवधिक तौर पर अद्यतन किया जाना चाहिए।

ग. सुरक्षा की संभावित दुर्बलताओं / उल्लंघनों की पहचान की जानी चाहिए। कार्यकलापों के पर्यवेक्षण और कर्तव्यों के पृथक्करण जैसे उपायों के द्वारा सूचना के संबंध में चोरी, धोखाधड़ी, त्रुटि और अनधिकृत परिवर्तनों के जोखिम को कम करने के लिए उपाय होने चाहिए।

घ. अनुप्रयोगों के संबंध में किन्हीं भी अनधिकृत प्रविष्टियों की अनुमति अनिवार्यतः नहीं दी जानी चाहिए जिन्हें डेटाबेस में अद्यतन किया जाना चाहिए। इसी प्रकार, किसी प्रविष्टि को अधिकृत करने के बाद कोई भी आशोधन करने की अनुमति अनिवार्यतः नहीं दी जानी चाहिए। कोई भी अनुवर्ती परिवर्तन अनिवार्यतः मूल प्राधिकृत प्रविष्टि को उलटने तथा एक नई प्रविष्टि करने के द्वारा ही किया जाना चाहिए।

ङ. अनुप्रयोग में सुदृढ़ वैधीकरण नियंत्रण, प्रसंस्करण और उत्पादन नियंत्रण निर्मित करने की आवश्यकता है। वैधीकरण सभी महत्वपूर्ण पृष्ठों पर शामिल किये जाने चाहिए ताकि आक्रमणों को न्यूनतम किया जा सके और स्रोत पर डेटा में परिवर्तन नहीं किया जा सके।

च. महत्वपूर्ण अनुप्रयोगों के संबंध में असफल लाग-आन प्रयासों के लागिंग, अनुप्रयोग में संवेदनशील विकल्पों, उदा. मास्टर अभिलेख परिवर्तन, प्रवेश अधिकार प्रदान करना, प्रणालीगत उपयोगी सेवाओं का प्रयोग, प्रणाली विन्यास में परिवर्तन, आदि के प्रवेश के लिए व्यवस्था की जानी चाहिए।

छ. अनुवर्ती लेखा-परीक्षाओं (आडिट ट्रायल्स) का भंडारण किन्हीं आंतरिक/ विनियामक/ सांविधिक अपेक्षाओं के अनुसार एक निश्चित अवधि के अनुसार करने की आवश्यकता है तथा यह सुनिश्चित किया जाना चाहिए कि उनमें कोई हेर-फेर नहीं किया जाए।

12.5 सुरक्षित विकास परिवेश

क. संस्थाएँ प्रणाली विकास और समन्वय प्रयासों के लिए सुरक्षित विकासपरिवेशों की स्थापना और उनका उपयुक्त रूप से संरक्षण करेंगे जो समूचे प्रणाली विकास जीवन-चक्र को समाविष्ट करेंगे।

ख. उक्त विकास, परीक्षण और उत्पादन परिवेशों को उचित रूप से वियोजित करने की आवश्यकता है, किन्हीं अपवर्जनों को आईएससी द्वारा समाप्त (साइन आफ़) करना होगा।

ग. **प्रवेश, कार्य के उत्तरदायित्वों के अनुरूप न्यूनतम विशेषाधिकार और "जानने की आवश्यकता" के आधार पर होना चाहिए।**

12.6 बाह्यस्रोतीकृत विकास

आईटी/व्यवसाय टीम को बाह्यस्रोतीकृत (आउटसोर्स्ड) प्रणाली विकास की गतिविधि की समीक्षा करनी चाहिए। संस्था **अनुप्रयोग प्रणाली विक्रेताओं से लिखित में अनुप्रयोग संपूर्णता विवरण** प्राप्त कर सकती है जो अनुप्रयोग के बारे में विक्रय के समय मालवेयर से मुक्त, किन्हीं स्पष्ट `बगों' से मुक्त, तथा (वितरित किये जा रहे अनुप्रयोग के वर्शन और किसी भी अनुवर्ती वर्शनों/किये गये आशोधनों के) कूट में किन्हीं गुप्त (कोवर्ट) माध्यमों से मुक्त, उपयुक्त स्तर की व्यवस्था से युक्त हो।

12.7 प्रणाली कार्यात्मकता और सुरक्षा परीक्षण

सुरक्षा की कार्यात्मकता का परीक्षण किया जाना चाहिए

क. यह सुनिश्चित करने के लिए सभी अनुप्रयोग प्रणालियों का परीक्षण कार्यान्वयन के दौरान कार्यात्मकता नियंत्रणों के संबंध में एक संतुलित तरीके से किया जाना चाहिए कि वे संस्था की व्यावसायिक नीतियों/नियमों को पूरा करती हैं।

ख. प्रणाली में सुदृढ़ प्रणाली आधारित नियंत्रण निर्मित करने की आवश्यकता है तथा इसके द्वारा किसी अयांत्रित नियंत्रण पर निर्भरता कम करने की आवश्यकता है।

ग. प्रारंभ में तथा प्रमुख परिवर्तन करने के दौरान ज्ञात असुरक्षितताओं की जाँच करने के लिए सुरक्षा नियंत्रणों हेतु सभी अनुप्रयोगों का परीक्षण किया जाना चाहिए।

घ. प्रणाली को चालू करने (लाइव) से पहले अनुवर्ती लेखा-परीक्षाओं (आडिट ट्रायल्स) और विशिष्ट क्षेत्रों के संबंध में स्पष्टता होनी चाहिए जिन्हें अनुवर्ती लेखा-परीक्षाओंके भाग के रूप में एवं इसके लिए अनुवर्ती लेखा-परीक्षा अथवा लाग निगरानी प्रक्रिया इसके लिए उत्तरदायी कार्मिकों सहित प्राप्त करने की आवश्यकता है।

12.8 अन्य

क. डेटाबेस में प्रत्यक्ष पश्चस्तरीय (बैक-एण्ड) अद्यतन परिवर्धनों (अपडेट्स) को अत्यावश्यक स्थितियों को छोड़कर अनुमति नहीं दी जानी चाहिए तथा केवल सुस्पष्ट

व्यावसायिक आवश्यकता के साथ एवं संबंधित नीति के अनुसार उचित प्राधिकरण के बाद ही अनुमति दी जा सकती है।

ख. निष्क्रियता की एक विशिष्ट अवधि के बाद उपयोगकर्ताओँ को लाग-आउट करने के लिए अनुप्रयोगों को संरूपण (कान्फिगरेशन) दिया जाना चाहिए।

ग. किसी अनधिकृत आशोधन को रोकने के लिए उपयुक्त इंटरफेस नियंत्रण विद्यमान होने चाहिए।

घ. अनुप्रयोग के लिए एक उपयुक्त सहायक (बैकअप) नीति स्थापित की जानी चाहिए।

13. साइबर सुरक्षा

उद्देश्यः बीमा क्षेत्र के लिए साइबर सुरक्षा और संबंधित जोखिमों का समाधान करने के लिए संस्थाओं में जागरूकता उत्पन्न करना और दिशानिर्देश उपलब्ध कराना।

13.1 संकटपूर्ण प्रणालियों और साइबर सुरक्षा घटनाओं का वर्गीकरणः

प्रणालियों का वर्गीकरण संकटपूर्णता और गंभीरता के आधार पर श्रेणियों में किया जाना चाहिए।

13.2 संस्था का साइबर आघात-सहनीयता कार्यक्रम

साइबर जोखिम द्वारा प्रस्तुत विभिन्न चुनौतियों का समाधान बीमाकर्ताओं और बीमा मध्यवर्तियों द्वारा एक व्यापक प्रतिक्रिया के साथ किया जाना चाहिए। उपयुक्त रूप में प्रबंधन का उच्चस्तरीय ध्यान एक आवश्यकता है, क्योंकि एक प्रभावी सरकारी संरचना को साइबर सुरक्षा घटनाओं को समझने, उनका निवारण करने, उन्हें पहचानने, उनके संबंध में प्रतिक्रिया व्यक्त करने और उनका समाधान करने के लिए समर्थ होना चाहिए। इसके अतिरिक्त, साइबर आघात-सहनीयता सर्वोत्तम प्रथाओँ के साथ सुसंगत एक सुचारु रूप से कार्यरत साइबर सुरक्षा प्रबंध कार्यक्रम विद्यमान होना चाहिए और इसका सत्यापन पर्यवेक्षी समीक्षा के द्वारा किया जाना चाहिए। जैसा कि नीचे वर्णित है, प्रतिक्रिया का यह स्तर बीमा के मुख्य सिद्धांतों के साथ सुसंगत है।

प्रभावी होने के लिए साइबर सुरक्षा का समाधान किसी संस्था के सभी स्तरों पर किये जाने की आवश्यकता है। सामान्यतः किसी भी साइबर सुरक्षा कार्यक्रम में सम्मिलित है, निरंतर प्रक्रिया और नियंत्रण में सुधार, घटना प्रबंध प्रक्रियाएँ जैसे प्रतिक्रिया और आपदा समुत्थान, नवीनतम नेटवर्क नीतियाँ और क्रियाविधियाँ, प्रयोक्ता विशेषाधिकारों का कठोर प्रबंध और नियंत्रण, सुरक्षित संरूपण (कान्फिगरेशन) संबंधी मार्गदर्शन, उपयुक्त मालवेअर सुरक्षा प्रक्रियाएँ, हटाने योग्य मीडिया उपयोग का सुसंगत नियंत्रण, चल और गृह कार्यचालन प्रक्रियाओं की निगरानी, तथा सभी कार्मिकों के लिए निरंतर जागरूकता और शैक्षिक पहलें।

सामान्य रूप से यह स्वीकृत है कि साइबर आघात-सहनीयता के लिए सर्वोत्तम प्रथाओं में निम्नलिखित मुख्य क्षेत्र शामिल होने चाहिए, परन्तु जो इन्हीं तक सीमित नहीं हैं :

13.3 अभिनिर्धारण

क. अभिनिर्धारण से उन संकटपूर्ण आस्तियों, व्यावसायिक कार्यों और प्रक्रियाओं की पहचान करना अभिप्रेत है जिन्हें संकट के विरुद्ध संरक्षित किया जाना चाहिए।

ख. सूचना संबंधी आस्तियाँ (संवेदनशील व्यक्तिगत सूचना सहित) और संबंधित प्रणालीगत प्रवेश उक्त अभिनिर्धारण प्रक्रिया का भाग होने चाहिए।

ग. व्यवसाय प्रक्रिया अथवा विक्रेता जोखिम का अभिनिर्धारण किया जाना चाहिए और उसका मूल्यांकन प्रवेश (आन-बोर्डिंग) और परिचालन प्रक्रिया का अंग होना चाहिए।

घ. नियमित समीक्षाएँ और अद्यतनीकरण मुख्य घटक हैं, क्योंकि साइबर जोखिम निरंतर विकसित हो रहा है तथा `गुप्त जोखिम' उभर सकते हैं।

13.4 **संरक्षण**

क. नियंत्रण अग्रणी तकनीकी मानकों के अनुरूप होने चाहिए। आघात-सहनीयता अभिकल्प के द्वारा दिया जा सकता है। व्यापक संरक्षण के लिए अंतर-संबंधों तथा आंतरिक और बाह्य आशंकाओं के लिए प्रवेश के अन्य साधनों का संरक्षण आवश्यक है। संरक्षण का अभिकल्पन करते समय "मानवीय तत्व" पर विचार किया जाना चाहिए। अतः प्रशिक्षण भी साइबर जोखिम के विरुद्ध सुरक्षा जाल का एक अत्यावश्यक भाग है। बाह्यस्रोतीकृत कार्यकलापों के लिए उपयुक्त मात्रा में सूचना प्रौद्योगिकी (आईटी) नियंत्रणों को सुनिश्चित किया जाएगा।

ख. पोर्टलों की उपलब्धता का तत्व संविदाकरण और स्रोतीकरण का भाग होना चाहिए। डीडीओएस सदिशों (वेक्टरों) से संरक्षण के लिए स्रोतीकरण और निगरानी का अंग होने की आवश्यकता है।

ग. न्यूनतम विशेषाधिकारों के आधार पर प्रतिबंध के साथ उपयुक्त प्रवेश नियंत्रण को अनुप्रयोग और प्रवेश नियंत्रण अभिकल्प का भाग होना चाहिए।

13.5 पहचान

संकटपूर्ण प्रणालियों के लिए साइबर सुरक्षा निगरानी अत्यावश्यक है, क्योंकि सुरक्षा घटनाओं की निगरानी और / या विश्लेषण-विज्ञान से साइबर घटनाओं की पहचान और उनका न्यूनीकरण करने में सहायता मिलती है। इनमें अन्य पक्ष प्रदाताओं को शामिल किया जा सकता है।

13.6 प्रतिक्रिया और समुत्थान

साइबर घटनाओं का अभिज्ञान करना और उन्हें रोकना उनके घटित होने से पहले हमेशा संभव नहीं है, भले ही सर्वोत्तम प्रक्रियाएँ लागू की जाएँ। इस कारण से घटना के प्रति प्रतिक्रिया की आयोजना अत्यंत महत्व की है। सेवाओं का पुनरारंभ (यदि बाधित हों) घटनाओं के प्रभाव और सेवा की गंभीरता के आधार पर एक उचित समय-सीमा के अंदर किया जाना चाहिए। आकस्मिकता का आयोजन, अभिकल्पन, और व्यवसाय का समन्वयन एवं डेटा की संपूर्णता (डेटा साझेदारी के करारों के मामले में भी) शीघ्र पुनरारंभ के लिए मुख्य समर्थकारी हैं। आकस्मिकता के आयोजन को प्रभावी बनाने के लिए, एक नियमित परीक्षण होने की सिफारिश की जाती है। जाँच-पड़ताल को सुसाध्य बनाने के लिए न्यायिक तैयारी अत्यावश्यक है।

13.7 परीक्षण

परीक्षण कार्यक्रम, असुरक्षितता निर्धारण और व्यापन जाँच, परीक्षण के चरण में आधार हैं। परीक्षण शामिल किया जाना चाहिए जब प्रणालियाँ विनिर्दिष्ट की जाती हैं, विकसित की जाती हैं और एकीकृत की जाती हैं।

13.8 परिस्थितिगत जागरूकता

साइबर आशंकाओं की पहचान करने में जागरूकता का योगदान है। तदनुसार, एक आशंका आसूचना प्रक्रिया की स्थापना साइबर जोखिम को कम करने में सहायता करती है। इस संबंध में संस्थाओं को स्थापित सूचना साझेदारी पहलों में सहभागिता करनी चाहिए।

13.9 जानकारी और रिपोर्टिंग

संस्थाओं को साइबर सुरक्षा प्रबंध की प्रभावात्मकता का निरंतर पुनर्मूल्यांकन करना चाहिए। साइबर वृत्तांतों और घटनाओं से प्राप्त जानकारी सुधारित आयोजना में योगदान करती है। प्रौद्योगिकी में नई प्रगति की निगरानी की जानी चाहिए।

साइबर सुरक्षा घटनाएँ जो व्यावसायिक परिचालनों और बड़ी संख्या में ग्राहकों को गंभीर रूप से प्रभावित करती हैं, मालूम होने पर अधिकतम 48 घंटों की अवधि के अंदर आईआरडीएआई को सूचित की जानी चाहिए।

जहाँ महत्वपूर्ण सूचना की गोपनीयता, अखंडता, अथवा उपलब्धता संभवतः जोखिम में हों, वहाँ संस्थाओं को चाहिए कि वे सूचना सुरक्षा घटनाओं की रिपोर्ट अनिवार्यतः आईआरडीएआई और सर्ट-फिन को अपेक्षित डेटा तत्वों, एवं किसी अन्य उपलब्ध सूचना के साथ संस्था की सूचना सुरक्षा टीम, सुरक्षा परिचालन केन्द्र (एसओसी), अथवा सूचना प्रौद्योगिकी विभाग द्वारा अभिनिर्धारित किये जाने से **48 घंटों के अंदर** दें। कुछ मामलों में, रिपोर्टिंग करने से पहले संपूर्ण और प्रमाणीकृत सूचना की विद्यमानता व्यवहार्य नहीं हो सकती। संस्थाओं को सूचना देते समय अपना सर्वोत्तम अनुमान देना चाहिए तथा अद्यतन सूचना रिपोर्ट करनी चाहिए जैसे ही वह उपलब्ध हो।

14. प्लेटफार्म/ बुनियादी व्यवस्था की सुरक्षा

उद्देश्यः सर्वरों, अनुप्रयोगों, तथा नेटवर्क और सुरक्षा साधनों सहित, संस्था की सूचना प्रौद्योगिकी (आईटी) की बुनियादी व्यवस्था का संरूपण (कान्फिगरेशन) किया जाएगा जिससे सुरक्षा, विश्वसनीयता और स्थिरता को सुनिश्चित किया जा सके।

14.1 सुरक्षित विन्यास दस्तावेज और आवधिक निर्धारण

विन्यास (कान्फिगरेशन) सुरक्षित विन्यास दस्तावेजों (एससीडी) के आधार पर होगा। संस्था ओईएम की सिफारिशों और उद्योग की सर्वोत्तम प्रथाओं के आधार पर आधार-रेखा एससीडी को विकसित करेगी। एससीडी घटकों की निम्नलिखित सूची (परन्तु जो इन्हीं तक सीमित नहीं है) के लिए तैयार किये जाने चाहिए।

- परिचालन प्रणालियाँ (सर्वर और अंतिम स्थान - लैपटाप, डेस्कटाप)
- वेब सर्वर साफ्टवेयर (टामकैट, आईआईएस, अपाचे एचटीटीपी, आईबीएम एचटीटीपी और ओरकल एचटीटीपी, आदि)
- अनुप्रयोग सर्वर साफ्टवेयर (वेबलाजिक, आदि)
- डेटाबेस सर्वर (ओरकल, एमएस-एसक्यूएल, माईएसक्यूएल, पोस्टग्रेएसक्यूएल, आदि)
- नेटवर्क घटक (रूटर, वायरलेस प्रवेश पाइंट, आदि)
- सुरक्षा साधन (फायरवाल, वीपीएनएस, आईडीएस, आईपीएस, आदि)
- वायरलेस

एससीडी की समीक्षा प्रचलन के लिए सूचना सुरक्षा टीम द्वारा एक आवधिक आधार पर की जानी चाहिए। कुछ व्यावसायिक आवश्यकताओं/सीमाओं के कारण एससीडीएस में यथासंस्तुत विन्यासों के लिए अपवर्जनों का अनुमोदन पर्याप्त जोखिम निर्धारण के बाद औपचारिक अपवर्जन प्रक्रिया के द्वारा किया जाना चाहिए।

आईटी बुनियादी व्यवस्था आवधिक आधार पर परिभाषित एससीडीएस की तुलना में विन्यास समीक्षा (असुरक्षितता निर्धारण/व्यापन परीक्षण) के अधीन होनी चाहिए।

नियमित नियत निर्धारण, जैसे आंतरिक और बाह्य असुरक्षितता स्कैन, आईटी बुनियादी व्यवस्था के लिए संचालित किये जाने चाहिए जिनमें साफ्टवेयर, अनुप्रयोग, सर्वर, नेटवर्क, डेटाबेस, परिचालन प्रणाली, वायरलेस साधन, और अन्य नेटवर्क उपस्कर शामिल हैं, परन्तु जो इन्हीं तक सीमित नहीं हैं।

असुरक्षितता निर्धारण की आवृत्ति सूचना आस्ति (अनुप्रयोग, साफ्टवेयर, डेटाबेस, परिचालन प्रणाली, नेटवर्क साधन और वायरलेस नेटवर्क) की गंभीरता पर निर्भर होगी। सभी इंटरनेट अभिमुख अनुप्रयोगों के लिए उत्पादन परिवेश में नियोजन से पहले असुरक्षितता निर्धारण किये जाएँगे।

14.2 **संग्रथन (पैच) प्रबंध**

संस्था की बुनियादी व्यवस्था को सुरक्षा पैचों और कोटि-उन्नयन पैचों सहित, समर्थित, परीक्षित और उचित रूप से नवीनतम ओएस और डेटाबेस संग्रथनों (पैचों) के साथ अद्यतन किया जाना चाहिए। सिफारिश किये गये नये संग्रथनों (पैचों) के लिए, उत्पादन परिवेश में

उन्हें नियोजित करने से पहले प्रभाव विश्लेषण और परीक्षण निष्पादित किये जाएँगे। प्रतिकूल प्रभाव अथवा व्यावसायिक अनुप्रयोगों की अनुपलब्धता के लिए कारणभूत संग्रथनों (पैचों) के लिए, अपवर्जन अनुमोदन दस्तावेजों का अनुरक्षण भावी संदर्भ और संपरीक्षण के प्रयोजनों के लिए किया जाना चाहिए।

अंतिम स्थानों के लिए संग्रथनों (पैचों) का परीक्षण प्रयोक्ता मशीनों पर कार्यन्वित करने से पहले परीक्षण परिवेश में किया जा सकता है।

15. नेटवर्क सुरक्षा

उद्देश्यः समूची संस्था में उसके नेटवर्क के माध्यम से प्रेषित सूचना का संरक्षण पर्याप्त नेटवर्क सुरक्षा साधन नियोजित करने के द्वारा किया जाएगा।

नीति, प्रक्रियाएँ और दिशानिर्देशः

क. नेटवर्क को कार्य और संभवतः स्थान के आधार पर क्षेत्रों (जोन)/उप-नेटों में विभक्त किया जाएगा। प्रत्येक क्षेत्र/उप-नेट का आगे और विभाजन व्यवसाय और सुरक्षा की आवश्यकताओं के आधार पर अलग वीएलएएनएस में किया जा सकता है।

ख. सभी नेटवर्क साधनों का दृढ़ीभवन उत्पादन में नियोजित करने से पहले उनके संबंधित सुरक्षा विन्यास दस्तावेजों के आधार पर किया जाना चाहिए।

ग. नेटवर्क संरचना में तर्कसंगत स्थिति को यह सुनिश्चित करना चाहिए कि फायरवाल को उपमार्ग (बाईपास) से नहीं गुजरना चाहिए। इन नेटवर्कों के माध्यम से गुजरनेवाले इंटरनेट यातायात को आगे और नियंत्रित करने के लिए आईडीएस/आईपीएस समाधान के स्थानन के द्वारा गहन सुरक्षा (डिफेंस-इन-डेप्थ) कार्यान्वित किया जाएगा। इन समाधानों को आशंकाओं के वर्तमान हस्ताक्षरों/विशेषताओं के साथ नियमित रूप से अद्यतन किया जाएगा।

घ. अविश्वस्त नेटवर्क (इंटरनेट/अतिरिक्त नेट) पर संस्था के नेटवर्क संसाधनों के लिए दूरस्थ प्रवेश को समग्र नेटवर्क सुरक्षा प्रबंध में एकीकृत किया जाएगा।

ङ. किसी संस्था अथवा सुरक्षा क्षेत्र के अंदर सभी संबंधित सूचना प्रसंस्करण प्रणालियों की घड़ियाँ एक सहमति-प्राप्त सही समय-स्रोत के साथ समकालिक की जाएँगी।

च. यह सुनिश्चित करने के लिए कि कंप्यूटर संबंध और सूचना प्रवाह व्यावसायिक अनुप्रयोगों की प्रवेश नियंत्रण प्रणाली का उल्लंघन नहीं करें, नेटवर्कों के लिए मार्ग-निर्धारित (रूटिंग) नियंत्रण लागू किये जाने चाहिए।

छ. नेटवर्क साधनों के लिए विन्यासों के अनुमोदन और कार्यान्वयन हेतु कर्तव्यों का पृथक्करण होना चाहिए।

ज. नेटवर्क लिंकों और नेटवर्क साधनों के लिए पर्याप्त अतिरिक्त व्यवस्था की जानी चाहिए। अतिरिक्त नेटवर्क लिंकों और साधनों के लिए सुरक्षा का वही स्तर होना चाहिए जो प्राथमिक लिंकों के लिए है। **संस्था के नेटवर्क के अंदर विफलता के सभी एकल बिन्दुओं का अभिनिर्धारण किया जाएगा और इस प्रकार के अभिकल्प में जोखिमों का निर्धारण किया जाएगा।** जहाँ संभव हो, वहाँ नेटवर्क की विफलता का समाधान करने के लिए विफलता संबंधी (फेलओवर) प्रौद्योगिकियाँ उपलब्ध होनी चाहिए। नेटवर्क आरेख (डायग्रैम) (वायरलेस नेटवर्क सहित) प्रलेखीकृत किया जाएगा और उसे अद्यतन रखा जाएगा।

झ. महत्वपूर्ण नेटवर्क साधन संगृहीत किये जाएँगे तथा आशंकाओं और अपवर्जनों की पहचान करने के लिए उनका विश्लेषण किया जाएगा। आशंकाओं के प्रति तत्काल प्रतिक्रिया देने के लिए एक सुरक्षा परिचालन केन्द्र (एसओसी) के माध्यम से नेटवर्क सुरक्षा की निगरानी की जाएगी।

16. बीज-लेखन और कुंजी प्रबंध

उद्देश्यः जहाँ भी आवश्यक हो वहाँ संस्था बीज-लेखन (क्रिप्टोग्रफी) के माध्यम से सूचना की गोपनीयता, प्रामाणिकता और संपूर्णता का संरक्षण करेगी। बीज-लेखन की कुंजियों का उपयोग करते हुए किये गये संरक्षण का स्तर उस परिवेश के साथ सूचना के उपयोग की संवेदनशीलता और आवृत्ति के अनुरूप होगा जहाँ वह स्थित है/प्रयुक्त है।

नीति, प्रक्रियाएँ और दिशानिर्देशः

16.1 **कुंजियों संबंधी सामान्य निदेश**

क. डिजिटल हस्ताक्षर/प्रमाणपत्र भारत के प्रमाणीकरण प्राधिकारियों के नियंत्रक (सीसीए) द्वारा लाइसेंसीकृत प्रमाणीकरण प्राधिकारी (सीए) से प्राप्त किये जाएँगे।

ख. आंतरिक सीए के मामले में मास्टर चाबियों के प्रबंध के लिए उत्तरदायित्व / जिम्मेवारी का समनुदेशन औपचारिक रूप से संस्था के अंदर किया जाएगा।

ग. मुख्य अभिरक्षकों को अनिवार्यतः अपनी भूमिका के लिए जागरूक बनाया जाना चाहिए तथा वे चाबियों की सुरक्षा का प्रबंध करने में अपने दायित्वों को औपचारिक रूप से स्वीकार करेंगे।

घ. सममित (सिमेट्रिक) / असममित (ऐसिमेट्रिक) चाबी युग्म के उत्पादन के लिए मास्टर चाबियाँ ऐसे तरीके से सुरक्षित रखी जानी चाहिए कि जहाँ भी लागू हो, वहाँ समूची मास्टर चाबी के प्रति कोई एक वैयक्तिक पक्षकार संबंधित (प्रिवी) न हो।

ङ. जब भी कोई जोखिम घटित होता है (अथवा घटित होने का विचार उत्पन्न होता है), तथा जब भी कोई पक्षकार जो चाबी / चाबियों के जोड़े के निजी चाबी घटक के लिए संबंधित (प्रिवी) है, संस्था को छोड़ देता है अथवा भूमिका बदलता है, तब चाबियाँ / असममित (ऐसिमेट्रिक) चाबियों के जोड़े बदले जाएँगे। सममित चाबियों / असममित चाबियों के जोड़ों का एक सामयिक और प्रभावी तरीके से प्रतिसंहरण करने के लिए एक औपचारिक प्रक्रिया अवश्य विद्यमान होनी चाहिए। प्रतिसंहरित चाबियाँ नष्ट की जाएँगी।

च. चाबी बैकअप प्रक्रिया चाबी को पुनः प्राप्त करने में समर्थ बनाएगी, परन्तु इससे चाबी की गोपनीयता और संपूर्णता को जोखिम में नहीं डालना चाहिए। चाबियाँ / चाबियों के जोड़े पुनः प्राप्त करने के लिए अनुरोध एक ऐसी औपचारिक प्रक्रिया के माध्यम से किया जाएगा, जो सक्षम प्राधिकारी से अनुमोदन को शामिल करती है।

16.2 **इलेक्ट्रानिक चाबियों का प्रतिधारण**

- डेटा बीज-लेखन चाबियाँ - बीज-लेखन के लिए प्रयुक्त सममित / असममित चाबियाँ तब तक उपलब्ध होंगी जब तक उक्त चाबियों के द्वारा संरक्षित (बीज-लिखित) किसी सूचना को खोलने की आवश्यकता हो।
- डिजिटल प्रमाणपत्र का सत्यापन - एक सार्वजनिक चाबी तब तक उपलब्ध होगी जब तक संबद्ध निजी चाबी से हस्ताक्षर की गई कोई भी सूचना अनुरक्षित की जाती है।
- अन्य चाबियाँ व्युत्पन्न करने के लिए प्रयुक्त मास्टर चाबी - मास्टर चाबियाँ तब तक उपलब्ध होंगी जब तक व्युत्पन्न चाबियाँ भविष्य में पुनः निर्मित करने की आवश्यकता हो।
- हैश ऐल्गरिदमों को उत्पन्न करने के लिए प्रयुक्त चाबियाँ - हैश ऐल्गरिदमों को उत्पन्न करने के लिए प्रयुक्त चाबियाँ तब तक उपलब्ध होंगी जब तक पूर्व में उत्पन्न किये गये हैश मूल्य की विधिमान्यता को प्रमाणित करने या अन्य प्रकार की स्थिति जानने की आवश्यकता हो।

17. **सुरक्षा लागिंग और निगरानी**

उद्देश्यः सामयिक तरीके से सुरक्षा संबंधी घटनाओं का पता लगाने के लिए संस्थाएँ लागिंग और निगरानी की क्षमताएँ स्थापित करेंगी।

नीति, क्रियाविधियाँ और दिशानिर्देश

17.1 लागिंग और निगरानी

क. सभी संकटपूर्ण सूचना आस्तियों पर सुरक्षा लाग सक्षम किये जाएँगे। लागिंग और निगरानी (एसओसी व्यवस्था) के प्रति एक केन्द्रीयकृत दृष्टिकोण लागू किया जाना चाहिए।

ख. विभिन्न प्रणालियों और साधनों के द्वारा उत्पन्न किये गये सुरक्षा लाग इस प्रकार से प्राप्त किये जाने चाहिए कि इन सभी प्रणालियों और साधनों के जरिये उत्पन्न घटनाओँ का योजन (सहसंबंध) संभव हो तथा उसका अनुरक्षण छह महीने की न्यूनतम अवधि के लिए किया जाना चाहिए और यथाप्रयोज्य रूप में अन्य विशिष्ट विनियामक शर्तें पूरी की जानी चाहिए।

ग. सुरक्षा लाग जब भी आवश्यक हो तब विधि प्रवर्तन अभिकरणों, आईआरडीएआई और सर्ट-फिन (सीईआरटी-एफआईएन) को उपलब्ध कराये जाएँगे।

घ. संकटपूर्ण प्रणालीगत कार्यकलापों का पता लगाने के लिए लागिंग को समर्थ बनाया जाएगा, जिनमें शामिल होंगेः

- प्रयोक्ता लेखा प्रबंध
- विशेष सुविधा प्राप्त प्रयोक्ता के कार्यकलाप
- ओएस विन्यास (कान्फिगरेशन) में परिवर्तन
- बहुविध अधिप्रमाणन विफलताएँ / समकालिक लाग-इन
- संपरीक्षण खोज में प्रवेश

ङ. अनुप्रयोग, परिचालन प्रणाली, डेटाबेस, नेटवर्क और सुरक्षा साधनों सहित सभी सूचना प्रणालियाँ लाग की गई घटनाओँ का सही और पता लगाने योग्य अभिलेख उपलब्ध कराने के लिए एक मानक समय-उपकरण / सर्वर (एनटीपी) के साथ समय का समक्रमण (सिंक्रोनाइजेशन) बनाये रखेंगे।

च. लाग प्रतिधारण कार्यक्रम को संस्था की अभिलेख प्रतिधारण नीति का अनुपालन करना चाहिए। सभी लाग और लागिंग सुविधाओँ का संरक्षण किसी भी हस्तक्षेप और अनधिकृत पहुँच के विरुद्ध किया जाना चाहिए।

छ. निगरानी की रिपोर्टें प्रबंधन की आवश्यकताओं के आधार पर प्रकाशित की जानी चाहिए। पर्याप्तता और अंतर्वस्तुओं के लिए लागों और निगरानी रिपोर्टों की आवधिक समीक्षा निष्पादित की जानी चाहिए।

ज. सूचित की गई घटनाओं को परिभाषित समय-सीमाओं के अंदर समाप्त किया जाना चाहिए।

18. घटना प्रबंध

उद्देश्यः सूचना सुरक्षा को सुनिश्चित करना तथा साइबर सुरक्षा संबंधी घटनाओं और सूचना प्रणालियों से संबद्ध कमजोरियों को सूचित करना एवं एक सामयिक तरीके से सुधारात्मक कार्रवाइयाँ करना।

i. सूचना सुरक्षा और साइबर सुरक्षा घटना प्रबंध के लिए नीति, क्रियाविधियाँ और दिशानिर्देश तैयार किये जाएँगे तथा सूचना सुरक्षा घटनाओं और कमजोरियों का पता लगाने, उन्हें अभिलिखित करने, उनके प्रति प्रतिक्रिया व्यक्त करने, उनका उन्नयन करने और उनका निवारण करने के लिए उनका प्रभावी ढंग से कार्यान्वयन किया जाएगा।

ii. यह सुनिश्चित करने के लिए एक प्रणाली लागू की जानी चाहिए कि सूचना सुरक्षा घटनाएँ और सूचना आस्तियों के साथ संबद्ध कमजोरियाँ सूचित की जाएँ तथा एक सामयिक तरीके से सुधारात्मक कार्रवाइयाँ की जाएँ।

iii. संस्था के द्वारा एक घटना प्रबंध प्रक्रिया स्थापित की जाएगी, प्रलेखित की जाएगी, कार्यान्वित की जाएगी और अनुरक्षित की जाएगी। इसमें शामिल होंगे सुरक्षा घटना और दुर्बलताओं की पहचान, सूचना-प्रणाली, अभिलेखन, प्रतिक्रिया, पुनःप्राप्ति और न्यूनीकरण प्रक्रियाएँ। घटना प्रबंध प्रक्रिया के सभी हितधारकों की भूमिकाएँ और जिम्मेदारियाँ परिभाषित की जाएँगी।

iv. सभी घटना संबंधी निर्णय लेने के लिए घटना प्रबंध टीम स्थापित की जाएगी। एक संचार माध्यम की स्थापना आंतरिक पक्षकारों और बाह्य संगठनों (उदा. विनियमनकर्ता, मीडिया, विधि प्रवर्तन, ग्राहक) के साथ की जाएगी।

v. निगरानी प्रणाली विद्यमान होनी चाहिए ताकि सुरक्षा घटनाओं और अपक्रियाओं से बचने के लिए सक्रिय कार्रवाई की जा सके।

vi. सूचना सुरक्षा और साइबर सुरक्षा घटना वर्गीकरण मानदंड प्रलेखीकृत किये जाएँगे। गंभीरता और तीव्रता के आधार पर सुरक्षा घटनाओं का वर्गीकरण किया जाएगा।

vii. घटना के मूल कारण का निर्धारण करने तथा सुधारात्मक और निवारक उपायों की पहचान करने के लिए एक प्रक्रिया परिभाषित की जाएगी।

viii. घटना और साइबर संकट के लिए; एक व्यापक साइबर सुरक्षा प्रतिक्रिया योजना विकसित करने और उसकी सहायता लेने की आवश्यकता है।

ix. घटना और साइबर संकट के लिए; एक व्यापक साइबर संकट प्रबंध योजना (सीसीएमपी) विकसित करने और उसकी सहायता लेने की आवश्यकता है। संस्था के लिए साइबर आक्रमण रोकने तथा किसी भी साइबर-घुसपैठ का तत्काल पता लगाने के लिए प्रभावी उपाय करने की आवश्यकता होगी जिससे किसी घटना के

प्रति प्रतिक्रिया व्यक्त की सके / पुनःप्राप्ति की जा सके / नियंत्रण किया जा सके।

x. सीसीएमपी बनाते समय संस्थाओं के द्वारा सर्ट-इन/एनसीआईआईपीसी दिशानिर्देशों का संदर्भ लिया जाए।

18.1 **घटना का प्रतिवेदन तथा उन्नयन संभलाई प्रक्रियाएँ और क्रियाविधियाँ**

क. घटना की सूचना देने के लिए उपयुक्त प्रौद्योगिकी का अभिनियोजन तथा सामयिक उन्नयन और सूचित की गई घटनाओं के संबंध में कार्रवाई के लिए दिशानिर्देश और प्रक्रियाएँ।

ख. घटना प्रबंध के लिए लागिंग, वर्गीकरण, निरूपण (डायग्नोसिस) और सुधार प्रक्रियाएँ विस्तृत रूप में निर्धारित की जाएँगी।

ग. उच्च अथवा संकटपूर्ण के रूप में वर्गीकृत घटनाओं की सूचना सर्ट-इन और सर्ट-फिन सहित, सीआईएसओ, सीआईओ, सीआरओ और अन्य संबंधित हितधारकों को दी जानी चाहिए।

I. जानकारी के आधार की आवश्यकता, जो नई घटनाओं की तुलना लागिंग और समाधान की गई घटनाओं के साथ करने देती है।

II. सुरक्षा संबंधी जिन घटनाओं का ग्राहक सेवा पर ध्यान देने योग्य प्रभाव है अथवा जिन घटनाओं की सूचना किसी कानूनी, विनियामक और/ या सांविधिक अपेक्षा के तौर पर बाहरी संस्थाओं को देने की आवश्यकता है, उनकी सूचना केवल संबंधित पदनामित अधिकारी के द्वारा ही दी जानी चाहिए।

18.2 **निवारक और अभिज्ञापक नियंत्रणों की कार्यपद्धति की समीक्षा**

क. संस्थाओं से प्रत्याशित है कि वे उभरती साइबर आशंकाओं, जैसे `शून्य दिन' (जीरो डे) आक्रमण, दूरस्थ प्रवेश आशंकाएँ, और लक्ष्यित आक्रमण, का सामना करने के लिए भली भाँति तैयार रहें।

ख. घटना निगरानी प्रणालीः अभिनियोजित नियंत्रणों की प्रभावात्मकता की निगरानी, मापन और समीक्षा करने के लिए एक क्रियाविधि होनी चाहिए।

19. अंतिम स्थान (एण्ड पाइन्ट) सुरक्षा

नीति, प्रक्रियाएँ और दिशानिर्देशः सूचना प्रणाली की आधारभूत व्यवस्था में अंतिम स्थानों (एण्ड पाइन्ट्स) के लिए आशंकाओं का समाधान करने के लिए तथा अंतिम स्थानों में अनधिकृत प्रवेश को रोकने के लिए नीति, मानक, प्रक्रियाएँ और दिशानिर्देश विकसित किये जाएँगे।

19.1 **वस्तुनिष्ठ अंतिम स्थान सुरक्षा**

क. यह सुनिश्चित करना कि अंतिम स्थान के पास एक अद्यतन की गई संग्रथित (पैच्ड) परिचालन प्रणाली है तथा विषाणु-रोधी (ऐन्टी वाइरस) साफ्टवेयर नवीनतम विषाणु परिभाषाओं, आदि से युक्त है।

ख. यह सुनिश्चित करना कि प्रणालीगत संरूपण (कान्फिगरेशन) सही हैं तथा सुरक्षा की अपेक्षाओं के साथ कोई समझौता नहीं किया गया है।

ग. नेटवर्क में प्रवेश पाने से अनधिकृत बाहरी प्रयोक्ताओं और नेटवर्क यातायात को रोकना।

घ. अंतिम स्थान के साथ अनधिकृत साधनों और अन्य सुवाह्य (पोर्टबल) भंडारण साधनों को जोड़ने से रोकना।

ङ. अंतिम स्थानों पर किसी भी अनधिकृत साफ्टवेयर को रोकना/पहचानना।

च. तकनीकी प्रणाली और साफ्टवेयर असुरक्षितताओं का समाधान त्वरित रूप से और प्रभावी ढंग से करना।

छ. संगरोधित प्रणालियों / साधनों में क्षमता का निर्माण करना, यदि वे अनुपालन न करते हुए अथवा संक्रमित स्थिति में पाये जाते हैं।

19.2 **पहचान और अंतिम स्थानों पर प्रवेश**

क. संस्था के नेटवर्क में प्रवेश की अनुमति देने से पहले अंतिम स्थान उपकरण को संस्था की "स्वीकार्य उपयोग नीति" का अनुपालन करने की अनुमति दी जानी चाहिए।

ख. प्रयोक्ता अधिकार उनकी व्यावसायिक/ कार्यात्मक आवश्यकताओं के अनुसार न्यूनतम विशेषाधिकार के सिद्धांत के आधार पर आबंटित किये जाने चाहिए। प्रयोक्ता अधिकार "रखने की आवश्यकता" और "जानने की आवश्यकता" पर आधारित होने चाहिए।

19.3 नेटवर्क प्रवेश नियंत्रण

केवल प्राधिकृत प्रयोक्ताओं के प्रवेश को सुनिश्चित करने के लिए संस्था के वैन (डब्ल्यूएएन) अथवा बाह्य नेटवर्क से जुड़े हुए अंतिम स्थानों के लिए अधिप्रमाणन व्यवस्था को कार्यान्वित किया जाना चाहिए।

19.4 दूरस्थ प्रवेश

क. संस्था को दूरस्थ प्रवेश अनुमोदनों की नियमित रूप से समीक्षा करनी चाहिए तथा उन अनुमोदनों को वापस लेना चाहिए जिनके संबंध में अनिवार्य व्यावसायिक औचित्य न हो।

ख. संस्था को दूरस्थ प्रवेश उपकरणों पर विद्यमान सभी साफ्टवेयर का उपयुक्त और समय पर संग्रथन (पैचिंग), अद्यतनीकरण और अनुरक्षण सुनिश्चित करना चाहिए।

ग. प्रवेश उपकरण और संस्था के बीच महत्वपूर्ण डेटा के संदेशों का संरक्षण करने के लिए कूटलेखन (एन्क्रिप्शन) का प्रयोग किया जाना चाहिए।

घ. संस्था के अंदर प्राधिकृत नेटवर्क क्षेत्रों और अनुप्रयोगों में दूरस्थ प्रवेश को प्रतिबंधित करने के लिए वीएएलएनएस, नेटवर्क खंडों, निर्देशिकाओँ और अन्य तकनीकों का प्रयोग किया जाना चाहिए।

ङ. टीसीपी/आईपी इंटरनेट-आधारित दूरस्थ प्रवेश का प्रयोग करते समय, संस्था के लिए इस सार्वजनिक बुनियादी व्यवस्था पर सुरक्षित रूप में डेटा पैकेट संप्रेषित करने के लिए इंटरनेट पर एक वीपीएन/उपयुक्त संचार माध्यम स्थापित करने की आवश्यकता है।

19.5 अनुप्रयोग नियंत्रण

क. संस्था आशंका के कारण, आक्रमण सदिश (वेक्टर) और सुरक्षा संबंधी दुर्बलता के साथ संबद्ध संभावना का आकलन कर सकती है तथा उसे संस्था के तकनीकी और व्यावसायिक प्रभाव के अनुमान के साथ संबद्ध कर सकती है।

ख. संस्था के स्वामित्व में स्थित सभी अंतिम स्थान/कार्यस्थान पूर्व-अनुमोदित लाइसेंसप्राप्त साफ्टवेयर के साथ संपन्न किये जाएँगे। वैयक्तिक अथवा कार्यालयीन उपयोग के लिए कार्यस्थान में गैर-मानक साफ्टवेयर का कोई भी अनधिकृत संस्थापन निषिद्ध किया जाना चाहिए।

19.6 **साधन नियंत्रण**

क. चल भंडारण साधन, जैसे यूएसबी, सीडी-रोम, आरडब्ल्यू-सीडी, बाह्य हार्ड ड्राइव, कैमरे, पोर्टबल मीडिया प्लेयर, कार्ड रीडर, मोबाइल फोन, आदि के उपयोग से उत्पन्न होनेवाले जोखिमों का नियंत्रण करने के लिए उपयुक्त नियंत्रण विद्यमान होने चाहिए।

ख. आईटी सहायता टीम को चाहिए कि वह सूचना सुरक्षा टीम द्वारा उपलब्ध कराये गये आधार-रेखा सुरक्षा संरूपण (कान्फिगरेशन) दस्तावेजों के अनुसार सभी अंतिम स्थान साधनों का संरूपण करे। लाइसेंसरहित अथवा संदिग्ध साफ्टवेयर अनुप्रयोगों का संस्थापन नहीं किया जाना चाहिए।

ग. जब भी लैन के साथ जोड़ा जाता है, तब यह अवश्य सुनिश्चित किया जाना चाहिए कि साधन पर नवीनतम संकेतों के साथ विषाणु-रोधक (ऐन्टी-वाइरस) एजेंट का संस्थापन किया जाए।

घ. संस्था उपयोगाधीन डेटा, गतिशील डेटा और शांत डेटा की पहचान, निगरानी और संरक्षण करने के लिए डेटा हानि निवारण (डीएलपी) जैसे सुरक्षा साफ्टवेयर का नियोजन करने पर विचार कर सकती है।

20. आभासीकरण

उद्देश्यः कंपनी के सूचना प्रौद्योगिकी (आईटी) बुनियादी व्यवस्था के अंदर आभासी परिवेश के उपयोग के दौरान सूचना के संरक्षण को सुनिश्चित करना।

नीति, प्रक्रियाएँ और दिशानिर्देशः प्रणालियों के आभासीकरण के लिए अनुमोदित नीति, प्रक्रियाएँ और दिशानिर्देश विद्यमान होंगे, जिनमें कम से कम निम्नलिखित का विवरण उपलब्ध होगाः

- आभासीकृत प्रणालियों का केन्द्रीकृत प्रबंध
- आभासीकृत यंत्र में विभिन्न प्रणालियों के बीच संसाधनों का प्रावधानीकरण और आबंटन
- मेजबान (होस्ट) और आभासीकृत यंत्रों में सूचना की सुरक्षा विद्यमान है

20.1 प्रवेश नियंत्रण

क. यह सुनिश्चित करने के लिए कि कोई अनधिकृत आभासी मेजबान अथवा मेहमान निर्मित न किये जाएँ, प्रवेश नियंत्रण कार्यान्वित किया जाएगा और पर्याप्त प्रक्रिया विद्यमान होगी। मेजबान से और मेजबान तक पहुँच की अनुमति एक फायरवाल के नियंत्रणों के माध्यम से होनी चाहिए जिससे पहुँच को केवल आवश्यक सेवाओं तक सीमित रखा जा सके।

ख. मेजबान ओएस के लिए नेटवर्क पहुँच को प्रबंध सेवाओं तक तथा यदि आवश्यक हो तो भंडारण तक सीमित कर देनी चाहिए।

ग. आभासी नेटवर्कों, आभासी सर्वरों और बैक अप के प्रबंध के लिए प्रबंधकीय पहुँच को अलग किया जाना चाहिए।

घ. मेजबान ओएस से मेहमान तक संदेशों को सुरक्षित रखा जाना चाहिए।

ङ. वीएम को केर्नेल या मेजबान द्वारा प्रयुक्त संसाधनों तक पहुँचने अथवा देखने में समर्थ नहीं होना चाहिए। इन संसाधनों में भंडारण और नेटवर्क शामिल हैं।

च. आभासी परिवेश प्रबंध कंसोल तक पहुँच संपरीक्षण (आडिट) लागिंग क्षमता से युक्त केन्द्रीकृत प्रबंधकीय कंसोल के माध्यम से होनी चाहिए।

छ. यदि उत्पाद और उत्पादेतर वीएमएस को एक ही मेजबान ओएस पर स्थान दिया जाता है, तो युक्तियुक्त पृथक्करण को सुनिश्चित करने के लिए पर्याप्त सुरक्षा नियंत्रण विद्यमान होने चाहिए।

20.2 परिचालन प्रणालियों का कठोरीकरण

क. फाइलों की अनधिकृत साझेदारी, समय के समक्रमण (सिंक्रोनाइजेशन) को रोकने के लिए, उपयुक्त कठोरीकरण को लागू किया जाना चाहिए।

ख. सभी अनावश्यक प्रोग्राम निकाल दिये जाएँगे (अन-इन्स्टाल किये जाएँगे) तथा सभी अनावश्यक सेवाएँ अक्षम कर दी जानी चाहिए।

ग. मेजबान ओएस को अवश्य नियमित रूप से और सामयिक ढंग से संग्रथित (पैच) किया जाना चाहिए, यह सुनिश्चित करने के लिए कि मेजबान ओएस द्वारा स्वयं प्रणाली का और मेजबान ओएसएस का संरक्षण उचित रूप से किया जा रहा है। इसके अतिरिक्त, संग्रथन (पैचिंग) की ये ही अपेक्षाएँ आभासीकरण साफ्टवेयर पर लागू होती हैं।

घ. वीएमएस का संरूपण (कान्फिगरेशन) डिफाल्ट से इस प्रकार किया जाएगा कि वे सहायक उपकरणों तक संबंधों को असमर्थ बना दें। सहायक उपकरणों तक संबंध अनुमोदित किये जाएँगे।

20.3 **विभाजन और संसाधन आबंटन**

खंडों (वाल्यूम्स) अथवा डिस्क विभाजन का उपयोग किया जाएगा तथा प्रत्येक आभासी मशीन पर कार्य-आधारित (रोल-बेस्ड) प्रवेश नियंत्रण अलग-अलग रूप से रखे जाने चाहिए।

20.4 **फाइल साझेदारी**

मेजबान ओएस फाइलों की अखंडता को रखने के लिए मेजबान और मेहमान के बीच फाइलों की साझेदारी की अनुमति नहीं दी जाएगी।

20.5 बैक अप

त्रुटियों के संबंध में पुनःप्राप्ति और परिचालनों की निरंतरता के लिए आभासी प्रणालियों को नियमित रूप से बैक-अप करने की आवश्यकता होगी।

20.6 **निगरानी**

यह सुनिश्चित करने के लिए कि वीएमएस के बीच कोई अनधिकृत परिचालन अथवा कोई दुर्भावपूर्ण परिचालन अथवा कोई संसाधनगत एकाधिकार घटित न हो, मेजबान और मेहमान के बीच परिचालनों की निगरानी करने हेतु उपयुक्त व्यवस्था विद्यमान होनी चाहिए।

21.**क्लाउड सुरक्षा**

उद्देश्यः यह सुनिश्चित करना कि क्लाउड संरचना पर संसाधित, संप्रेषित और भंडारण की गई सूचना सुरक्षित हो।

नीति, प्रक्रियाएँ और दिशानिर्देशः क्लाउड या किसी बाह्य मेजबानी की बुनियादी व्यवस्था पर रखी जानेवाली सूचना के प्रकार, उसके महत्व और अपनाये जानेवाले सुरक्षा नियंत्रणों के स्तर के लिए निर्देश देने हेतु नीति, प्रक्रियाएँ और दिशानिर्देश बनाये जाएँगे

- मुख्य व्यावसायिक अभिलेखों के इलेक्ट्रानिक अनुरक्षण के संदर्भ में, अभिलेख भारत के अंदर रखे जाएँगे।
- क्लाउड होस्टिंग माडल का चयन होस्ट की जा रही सूचना के महत्व पर निर्भर होगा।
- जहाँ भी क्लाउड में अनुप्रयोग/डेटा/प्रणाली के होस्टिंग को वाणिज्यिक, व्यावसायिक, विनियामक, विधिक अथवा अन्य कारणों से अपरिहार्य माना जाता है, वहाँ संस्था के द्वारा अपने संबंधित वरिष्ठ प्रबंधन से अनुमोदन प्राप्त करने चाहिए।
- क्लाउड में डेटा और प्रणाली को होस्ट करना अनिवार्य मानने के लिए व्यावसायिक औचित्य। क्लाउड पर होस्ट किये जानेवाले डेटा का वर्गीकरण उदा. गुप्त/अत्यधिक गोपनीय, गोपनीय, सार्वजनिक, आंतरिक, आदि।
- उसे निम्नलिखित को समाविष्ट करना चाहिएः
    - डेटा निःसरण/ डेटा करप्शन/ सुरक्षा भंग आदि के विरुद्ध रक्षा के लिए क्लाउड सेवा प्रदाता/ अनुप्रयोग सेवा प्रदाता/ किसी अन्य पक्षकार/ कंपनी द्वारा लागू किये जानेवाले सुरक्षा नियंत्रण उपाय एवं डेटा निःसरण सहित उल्लंघनों को रोकने, पहचानने और प्रतिक्रिया व्यक्त करने के लिए विद्यमान नियंत्रण उपाय।
    - उपयुक्त सेवा प्रदाता का चयन करने के लिए समुचित सावधानी प्रक्रिया।

21.1 **सेवा स्तरीय करार**

क. निम्नलिखित का समाधान करने के लिए एक उपयुक्त सेवा स्तरीय करार विद्यमान होगा

I. धारणीयता, विफलता से सुरक्षा परिचालनों के लिए समर्थन

II. डेटा पुनःप्राप्ति का समय, आईपीआर का संरक्षण, आदि

III. डेटा निःसरण और इसके प्रदर्शन सहित उल्लंघनों को रोकने, पहचानने और प्रतिक्रिया व्यक्त करने के लिए सुरक्षा नियंत्रण उपाय

IV. एकपक्षीय संविदा समाप्ति/निर्गम खंड

V. सूचना तक पहुँचने / लाग करने के लिए आईआरडीएआई / विधि प्रवर्तन एजेंसियों और सर्ट-फिन हेतु संपरीक्षण (आडिट) करने का अधिकार

ख. सेवा प्रदाता की संविदा में क्लाउड सेवाओं के माध्यम से संगृहीत, संसाधित और निपटाये गये डेटा की गोपनीयता, अखंडता, उपलब्धता और गुप्तता को सुनिश्चित करने के लिए खंड शामिल किये जाएँगे।

ग. सेवा प्रदाता के साथ संविदाओं में अन्य संविदागत अपेक्षा के अतिरिक्त निम्नलिखित को शामिल किया जाएगा, परन्तु जो इन्हीं तक सीमित नहीं होंगेः

i. एसएलए

ii. लागू विधियों और विनियमों का अनुपालन

iii. डेटा स्वामित्व

iv. अधिप्रमाणन नियंत्रण

v. लाग पुनःप्राप्तियाँ

vi. संग्रथन (पैच) प्रबंध

vii. संरूपण (कान्फिगरेशन) प्रबंध

viii. अनुप्रयोग/प्रणाली सुरक्षा परीक्षण

ix. डेटा पुनःप्राप्ति योजना

x. वियोजन अथवा संविदा की समाप्ति पर डेटा विलोपन

21.2 क्लाउड प्रवेश नियंत्रण

यह सुनिश्चित करने के लिए विश्वसनीय अधिप्रमाणन व्यवस्था के साथ उपयुक्त प्रवेश नियंत्रण व्यवस्था लागू की जाएगी

क. डेटा की साझेदारी क्लाउड पर अन्य ग्राहकों के साथ आकस्मिक तौर पर नहीं की जाएगी

ख. कर्तव्यों का तर्कपूर्ण विभाजन उपलब्ध कराने के लिए क्लाउड सेवा प्रदाता/ अनुप्रयोग सेवा प्रदाता/ किसी अन्य पक्ष कार्मिक के नियंत्रण विद्यमान हैं

ग. विशेषाधिकार पहुँच की लागिंग और निगरानी कार्यान्वित की जाएगी

21.3 क्लाउड डेटा सुरक्षा

क. सुरक्षित संरूपण (कान्फिगरेशन), अनुप्रयोग, ओएस, डीबी, वेब सर्वर, बैक-अप और पुनःप्राप्ति, परिवर्तन प्रबंध, क्षमता और माँग प्रबंध, दुर्भावपूर्ण कूट और निगरानी, क्लाउड पर संपरीक्षण (आडिटिंग) और लागिंग सुरक्षा की अपेक्षाओं को सुनिश्चित करने के लिए परिचालनों की सुरक्षा से संबंधित नियंत्रण कार्यान्वित किये जाएँगे।

ख. डी-इन-संक्रमण क्लाउड सूचना के वर्गीकरण के लिए उपयुक्त तौर पर कोडीकृत (एन्क्रिप्टेड) रूप में होगा।

ग. क्लाउड डेटा होस्टिंग के लिए कोडीकरण तकनीकें लागू की जाएँगी, जैसे पीआईआई के लिए मार्गस्थ डेटा और शांत डेटा।

घ. संस्था के लिए संवेदनशील डेटा की पहचान करने, निगरानी करने और संरक्षण करने तथा डेटा जोखिम का प्रबंध करने के लिए उपयुक्त डेटा हानि निवारण (डीएलपी) समाधान का उपयोग करने की सिफारिश की जाती है।

ङ. संस्था के द्वारा डेटा प्रतिधारण और नाशन कार्यक्रम परिभाषित किये जाने चाहिए तथा डेटा संरचनाओं में और मीडिया पर ढील (स्लैक) सहित सभी स्थानों पर समस्त डेटा को नष्ट करने पर विशेष बल के साथ अनुरोध किये जाने पर डेटा को नष्ट करने के लिए सेवा प्रदाता को जिम्मेदार बनाया जाना चाहिए।

च. डेटा प्रतिधारण नियंत्रण भी यह सुनिश्चित करें कि प्रतिधारण की समय-सीमा के बाद विभिन्न स्थानों पर भंडारण किये गये डेटा की बहुविध प्रतियाँ भी नष्ट की जाएँ।

22. गतिशील सुरक्षा

उद्देश्यः गतिशील संगणन साधनों और संचार सुविधाओं के उपयोग के साथ संबद्ध जोखिमों का प्रबंध करने के लिए उपयुक्त सुरक्षा उपायों के कार्यान्वयन के द्वारा दूरस्थ कार्य तथा मोबाइल साधनों का उपयोग करते समय सूचना आस्तियों की सुरक्षा को सुनिश्चित करना।

नीति, प्रक्रियाएँ और दिशानिर्देशः

मोबाइल संगणन के उपयोगकर्ताओं को निर्देश देने के लिए नीति, प्रक्रियाएँ और दिशानिर्देश तैयार किये जाएँगे ताकि कारपोरेट नेटवर्क सुरक्षित रहे।

नीति, प्रक्रियाओं और दिशानिर्देशों में निम्नलिखित भी शामिल होंगेः

क. बीवाईओडी (अपना स्वयं का साधन लाएँ) का उपयोग करते हुए संसाधित संस्था की सूचना और दूर-कार्य स्थलों के लिए सुरक्षा उपाय।

ख. श्रेणी "गतिशील साधनों" (मोबाइल डिवाइसेज़), जैसे मोबाइल फोन, स्मार्ट फोन, पोर्टबल साधन आदि, में आनेवाले साधनों का उपयोग करनेवाले सभी कर्मचारी, आंतरिक प्रशिक्षणार्थी (इन्टर्न्स) और बाह्य व्यक्ति मोबाइल साधनों का उपयोग करते हुए संस्था के नेटवर्क का उपयोग करने की अनुमति उन्हें देने से पहले उक्त सुरक्षा नीति और संबद्ध प्रक्रियाएँ और दिशानिर्देश स्वीकार करेंगे।

22.1 **अनुमोदित साधन / सेवाएँ**

क. प्रयोग में स्थित मोबाइल साधनों की एक सूची (इन्वेंटरी) रखी जानी चाहिए, चाहे वे संस्था के उपकरणों के स्वामित्व में हों या बीवाईओडी के, जिसके साथ स्वामित्वप्राप्त व्यक्ति का नाम और नेटवर्क प्रवेश नियंत्रण के लिए पहचान को अधिदेशात्मक बनाया जाना चाहिए। इस इन्वेंटरी में कम से कम अभिनिर्धारकों की सूची को हिसाब में लिया जाएगा, जैसे साधन का नाम, स्वामी का आईडी, साधन की क्रम संख्या, साधन का आईएमईआई, साधन का एमएसी पता, साधन की क्षमताएँ, आदि, जोकि केवल इन्हीं तक सीमित नहीं होगी।

ख. संस्था का आईटी विभाग प्राधिकृत अनुप्रयोगों की सूची तैयार करेगा तथा उसके पास ऐसी सूची के प्रबंध के संबंध में एक प्रलेखीकृत प्रक्रिया होगी। यह प्रक्रिया उपलब्ध नये साधनों/सेवाओं, साधनों की नई क्षमताओं और नई आशंकाओं को ध्यान में रखते हुए एक आवधिक आधार पर अनुमोदित अनुप्रयोगों एवं अनुमोदित साधनों/सेवाओं की समीक्षा व्यवस्था को समाविष्ट करेगी।

22.2 **घटना प्रबंध**

सुरक्षा संबंधी घटना का संदेह होने पर, विशेष रूप से जब किसी मोबाइल साधन के खो जाने या चोरी किये जाने पर तत्काल उपयुक्त प्राधिकारी को अधिसूचित किया जाएगा।

22.3 दूरस्थ अवरोधन और दूरस्थ मार्जन

क. साधनों की हानि/चोरी अथवा स्टाफ-सदस्य के नियोजन में परिवर्तन की स्थिति में डेटा का संरक्षण करने के लिए संस्था के आंतरिक नेटवर्कों में पहुँच रखनेवाले सभी साधनों के लिए दूरस्थ साधन के मार्जन अथवा अवरोधन की व्यवस्था को उपयुक्त रूप में कार्यान्वित किया जाना चाहिए।

ख. यदि साधनों का मूलोच्छेद किया गया हो अथवा वे बंधन-मुक्त (जेल-ब्रोकेन) हो गये हों, तो उद्यम के नेटवर्क में प्रवेश करने से साधनों को रोकने के लिए नियंत्रण विद्यमान होने चाहिए।

22.4 **नेटवर्क प्रवेश नियंत्रण**

क. मोबाइल साधनों / दूरस्थ कार्य को कारपोरेट सेवाओं तक पहुँचने के लिए आंतरिक नेटवर्क के साथ संबद्ध होने की अनुमति पूर्व-अनुमोदन से दी जाएगी।

ख. संस्था के नेटवर्क में मोबाइल साधनों / दूरस्थ कार्य को प्रवेश देने के लिए उपयुक्त सुरक्षा अधिप्रमाणन और प्राधिकृत करने की व्यवस्था लागू की जाएगी। बेतार (वायरलेस) संबद्धता की अनुमति केवल संस्था के अनुमोदित कूटलेखन (एन्क्रिप्शन) के साथ ही दी जाएगी।

22.5 मोबाइल डेटा सुरक्षा

क. मोबाइल साधन जिनमें सार्वजनिक सूचना को छोड़कर गोपनीय, वैयक्तिक, संवेदनशील और सामान्यतः कंपनी से संबंधित समस्त सूचना निहित हो, उक्त साधन में भंडारण किये गये कारपोरेट डेटा का संरक्षण करने के लिए कूटलेखन (एनक्रिप्शन) अथवा समान रूप से सुदृढ़ उपायों का नियोजन करेंगे।

ख. सभी मोबाइल साधन तथा कारपोरेट अनुप्रयोगों का प्रयोग करते हुए दूरस्थ कार्य में प्रयुक्त सभी सूचनागत आस्तियाँ संस्थापित और चालू विषाणु-रोधी और मालवेयर-रोधी साफ्टवेयर से युक्त होंगी।

23. **सूचना प्रणाली संपरीक्षण**

23.1 **संपरीक्षक की पात्रता और चयन**

सीआईएसए/ डीआईएसए/ पैनल में दर्ज संपरीक्षक में प्रमाणपत्र जैसे प्रमाणीकरण धारण करनेवाले अर्हता-प्राप्त बाह्य प्रणाली संपरीक्षक द्वारा स्वतंत्र आश्वासन संपरीक्षण किया जाएगा।

23.2 संपरीक्षण का विस्तार/प्रकारः

क) संपरीक्षण के विस्तार में इस दस्तावेज के साथ संलग्न अनुबंध के अनुसार परिभाषित नियंत्रण शामिल होंगे।

ख) वार्षिक आईएस संपरीक्षणों में पासवर्ड नियंत्रण, प्रयोक्ता आईडीएस का नियंत्रण, परिचालन प्रणाली सुरक्षा, मालवेयर-रोधी नियंत्रण, निर्माता-जाँचकर्ता नियंत्रण, पहचान

और प्रवेश प्रबंध, भौतिक सुरक्षा, अपवर्जन रिपोर्टों/संपरीक्षण खोजों की समीक्षा, बीसीपी नीति और परीक्षण आदि जैसे महत्वपूर्ण क्षेत्रों में, बड़ी और मध्यम शाखाओँ पर फोकस के साथ, नमूना आधार पर शाखाओं को भी समाविष्ट किया जाएगा।

ग) यह आश्वासन संपरीक्षण का संचालन सूचना सुरक्षा टीम द्वारा किया जाएगा।

23.3 **आवृत्तिः**

संपरीक्षण प्रत्येक वित्तीय वर्ष के लिए संचालित किया जाएगा।

23.4 आईएस संपरीक्षण का निष्पादन

संपरीक्षण के दौरान, संपरीक्षकों को चाहिए कि वे साक्ष्य प्राप्त करें, जाँच प्रक्रियाओं का निष्पादन करें, निष्कर्षों का उपयुक्त रूप से प्रलेखीकरण करें, तथा निष्कर्ष निकालकर एक रिपोर्ट बनाएँ।

23.5 **रिपोर्टिंग और अनुवर्ती कार्रवाइयाँ**

क. संपरीक्षकों के निष्कर्षों की उचित रिपोर्टिंग होनी चाहिए। इस प्रयोजन के लिए, प्रत्येक संस्था को एक संरचित फार्मेट तैयार करना चाहिए।

ख. संपरीक्षण के दौरान पाई गई बड़ी कमियों/विपथनों पर एक विशेष टिप्पणी में उल्लेख किया जाना चाहिए तथा तत्काल आईएससी और आईटी विभाग को दिया जाना चाहिए।

ग. संपरीक्षकों के द्वारा बताई गई छोटी अनियमितताओं को तत्काल सुधारा जाना चाहिए।

घ. संपरीक्षण रिपोर्टों पर अनुवर्ती कार्रवाई को उच्च प्राथमिकता दी जानी चाहिए तथा सुधारात्मक कार्रवाई कोई समय गँवाये बिना की जानी चाहिए।

ङ. संपरीक्षण रिपोर्टें बोर्ड की जोखिम प्रबंध समिति को प्रस्तुत करने की आवश्यकता है।

च. संपरीक्षण रिपोर्ट के कार्यात्मक सारांश की प्रति, की गई कार्रवाई के नोट के साथ आईआरडीएआई को संपरीक्षण के समापन से 30 दिन के अंदर प्रस्तुत की जानी चाहिए।

23.6 समीक्षा

संस्था को सूचित किया जाता है किः

क) संपरीक्षक के चयन और कार्यनिष्पादन की समीक्षा करे।

ख) सुनिश्चित करे कि संपरीक्षकों के कार्य को उचित रूप से प्रलेखीकृत किया गया है।
ग) संपरीक्षण रिपोर्टों के अनुवर्तन तथा आईएससी को तिमाही समीक्षा के प्रस्तुतीकरण के लिए उत्तरदायित्व ले।
घ) संपरीक्षकों का आवर्तनः तीन वर्ष में एक बार।

इस रिपोर्ट में विनिर्दिष्ट क्षेत्रों को समाविष्ट करते हुए एक नियंत्रण जाँच-सूची **अनुबंध क** में दी गई है।

24. सूचना और साइबर सुरक्षा संबंधी कानूनी संदर्भ

इस खंड में संस्थाओं को सूचना और साइबर सुरक्षा के लिए उपलब्ध विभिन्न सांविधिक उपबंधों के बारे में एक स्थूल विचार मिल सकता है। यहाँ संदर्भ के लिए सूचना प्रौद्योगिकी, साइबर सुरक्षा और सूचना की सुरक्षा के संबंध में उपलब्ध विभिन्न कानूनी उपबंधों को समेकित करने का प्रयास किया गया है। जबकि **अनुबंध ख** में दिये गये इन समेकित उपबंधों का उपयोग संदर्भ के लिए किया जा सकता है, इन्हें संपूर्ण नहीं समझा जाना चाहिए। संस्थाओं से अनुरोध है कि वे अद्यतन जानकारी / नवीनतम उपबंधों के लिए संबंधित अधिनियम/विनियम/नियमों/संशोधनों का संदर्भ लें।

****

अनुबंध खः सूचना और साइबर सुरक्षा के लिए कानूनी संदर्भ

सूचना और साइबर सुरक्षा

साइबर स्थान और साइबर कानून उभरती हुई प्रवृत्तियाँ हैं जहाँ तक कानूनी न्यायशास्त्र का संबंध है। पारंपरिक आफ़लाइन विषयों के असमान, जो समय के चलते विकसित हुए हैं और परिपक्व हुए हैं, साइबर कानून, कार्रवाई और संरक्षण विकसित होने के स्तर पर हैं। बड़ी सीमा तक आफ़लाइन विश्व का मूलभूत सिद्धांत आनलाइन विश्व में भी लागू होगा। तथापि, आनलाइन विश्व की जटिलताओँ के होते हुए, साइबर स्थान और आभासी विश्व की समस्याओं के साथ व्यवहार करने के लिए निश्चित रूप से विधि और विधिक प्रवर्तन की विशेष व्यवस्थाओँ की आवश्यकता है।

साइबर स्थान में लेनदेनों के कानूनी पहलुओं के चारों ओर परिभ्रमित करनेवाले महत्वपूर्ण विषय मुख्य रूप से निम्नलिखित के चारों ओर विकसित होंगेः

- ई-संविदाएँ और अधिप्रमाणन
- ई-हस्ताक्षर और डिजिटल हस्ताक्षर
- गुप्तता और डेटा संरक्षण
- डेटा प्रतिधारण और पुनःप्राप्ति
- इलेक्ट्रानिक साक्ष्य और स्वीकार्यता
- मध्यवर्ती दायित्व
- आईपी संरक्षण
- विवाद समाधान
- अधिकार-क्षेत्र और
- साइबर अपराध और प्रवर्तन

इंटरनेट विधियों और आनलाइन विश्व के साथ व्यवहार करने के लिए भारत का विधायी ढाँचा सूचना प्रौद्योगिकी अधिनियम, 2000 और उसके अधीन बनाये गये नियमों में सुरक्षित है। इसमें बाद में सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 द्वारा संशोधन किया गया। यह भारतीय दंड संहिता 1860, भारतीय साक्ष्य अधिनियम, 1872, बैंककार बही साक्ष्य अधिनियम, 1891 और भारतीय रिज़र्व बैंक अधिनियम, 1934 तथा संबंधित विषयों में संशोधन के लिए भी मार्ग प्रशस्त करता है।

उक्त आईटी अधिनियम और उसके अधीन विभिन्न नियमों ने इलेक्ट्रानिक डेटा के भंडारण, प्रसार, संसाधन और पुनःप्राप्ति के लिए कानूनी ढाँचा उपलब्ध कराया है। उक्त अधिनियम संवेदनशील वैयक्तिक डेटा और सूचना सहित, सूचना और डेटा को संभालते समय निगमित निकायों और बीमा मध्यवर्तियों द्वारा समुचित सावधानी संचालित करने के संबंध में दिशानिर्देश और दायित्व भी निर्धारित करता है। सरकारी प्राधिकारियों को साइबर सुरक्षा संबंधी घटनाओं की रिपोर्टिंग के लिए दायित्व भी विद्यमान हैं। इनका उल्लंघन करने से अपराधों और दंडों के लिए मार्ग प्रशस्त हो सकता है।

सूचना की परिभाषा आईटी अधिनियम के अंतर्गत बिलकुल व्यापक है और इसका अभिप्राय निम्नानुसार हैः

"सूचना" में शामिल हैं डेटा, संदेश, पाठ, प्रतिरूप (इमेज), ध्वनि, आवाज, कूट, कंप्यूटर प्रोग्राम, साफ्टवेयर और डेटाबेस या माइक्रो फिल्म या कंप्यूटर उत्पन्न माइक्रोफिश"।
आईटी अधिनियम के अंतर्गत यथापरिभाषित शब्द डेटा का अभिप्राय निम्नानुसार हैः

"डेटा" से अभिप्रेत है, सूचना, ज्ञान, तथ्यों, संकल्पनाओं या अनुदेशों का निरूपण जो तैयार किये जा रहे हैं अथवा औपचारिक तरीके से तैयार किये गये हैं, तथा संसाधित किये जाने के लिए उद्दिष्ट है, संसाधित किया जा रहा है अथवा किसी कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में संसाधित किया गया है एवं जो किसी भी रूप (कंप्यूटर प्रिंटआउटों, चुंबकीय या प्रकाशीय भंडारण मीडिया, पंच किये गये कार्ड, पंच किये गये टेप) में हो सकता है अथवा आंतरिक रूप से कंप्यूटर की मेमोरी में भंडारण किया गया है।

आईटी अधिनियम की धारा 2(एनबी) के अंतर्गत यथापरिभाषित शब्द "साइबर सुरक्षा" से अभिप्रेत हैः
"सूचना, उपकरण, साधन, कंप्यूटर, कंप्यूटर संसाधन, संचार साधन और अनधिकृत प्रवेश से उसमें भंडारण की गई सूचना, उपयोग, प्रकटीकरण, विघटन, आशोधन या नाशन से संरक्षण"।

साइबर अपराध दो स्थूल श्रेणियों में वर्गीकृत किये जा सकते हैं :

कंप्यूटर सहायता-प्राप्त साइबर अपराधः

स्पैम, फ़िशिंग, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, आनलाइन स्थान पर बौद्धिक संपत्ति उल्लंघन, अश्लील साहित्य, अनधिकृत प्रवेश कंप्यूटर सहायता-प्राप्त साइबर अपराधों के विशिष्ट उदाहरण हैं। यहाँ कंप्यूटर अपराध करने में सहायक है।

कंप्यूटर अभिमुख साइबर अपराधः

दुर्भावपूर्ण साफ्टवेयर का प्रयोग, त्रोजान, स्पाईवेयर, साइबर आतंकवाद, वर्म कंप्यूटर अभिमुख साइबर अपराधों के विशिष्ट उदाहरण हैं। यहाँ कंप्यूटर अपराध का लक्ष्य है।

वैयक्तिक सूचना का संरक्षण और उचित सुरक्षा व्यवहार

वैयक्तिक सूचना एवं आनलाइन विश्व में व्यवहार करनेवाले निगमित निकायों से यह सुनिश्चित करना अपेक्षित है कि वे उचित सुरक्षा व्यवहार और प्रक्रियाएँ बनाये रखें । जहाँ कोई निगमित निकाय, किसी कंप्यूटर संसाधन में जो उसके स्वामित्व में है, जिसका वह नियंत्रण करता है और जिसका परिचालन करता है, किसी संवेदनशील वैयक्तिक डेटा या सूचना जो उसके अधिकार में है, जिसका व्यवहार वह करता है और जिसे वह संभालता है, के संबंध में उचित सुरक्षा प्रथाओं और प्रक्रियाओं को लागू करने और बनाये रखने में उपेक्षा करता है, तथा इसके द्वारा किसी व्यक्ति के लिए अनुचित हानि अथवा अनुचित लाभ पहुँचाता है, वहाँ ऐसा निगमित निकाय इस प्रकार प्रभावित व्यक्ति को क्षतिपूर्ति के रूप में हर्जाने का भुगतान करने के लिए बाध्य होगा।

“उचित सुरक्षा प्रथाएँ और प्रक्रियाएँ” से अभिप्रेत है सुरक्षा प्रथाएँ और प्रक्रियाएँ जो ऐसी सूचना का संरक्षण अनधिकृत पहुँच, क्षति, उपयोग, आशोधन, प्रकटीकरण अथवा हानिकरण से करने के लिए अभिकल्पित हैं, जैसा कि पक्षकारों के बीच एक करार में विनिर्दिष्ट की जा सकती है अथवा फिलहाल प्रचलन में स्थित किसी कानून में विनिर्दिष्ट की जा सकती है तथा ऐसे करार या किसी कानून के अभाव में ऐसी उचित सुरक्षा प्रथाएँ और प्रक्रियाएँ जो केन्द्र सरकार द्वारा उसके द्वारा योग्य समझे जानेवाले व्यावसायिक निकायों या संघों के साथ परामर्श करने के बाद निर्धारित की जा सकती हैं।

इस संबंध में, सरकार ने सूचना प्रौद्योगिकी (उचित सुरक्षा व्यवहार और प्रक्रिया तथा संवेदनशील वैयक्तिक डेटा अथवा सूचना) नियम, 2011 अधिसूचित किये हैं।

उपर्युक्त नियमों के अनुसरण में, कोई भी संवेदनशील वैयक्तिक डेटा या सूचना पर स्वामित्व रखनेवाले, व्यवहार करनेवाले या उसे संभालनेवाले निगमित निकायों से अपेक्षित है कि वे अनुपालन की निम्नलिखित अपेक्षाओँ का पालन करें :

मुख्य दायित्व और पालन

निम्नलिखित सारणी में मुख्य अपेक्षाएँ तथा एसपीडीआई नियमों के अनुपालन के लिए कार्रवाई योग्य बातें सूचीबद्ध की गई हैं

दायित्व	**कार्रवाई योग्य बातें**
सूचना की गोपनीयता और प्रकटीकरण के लिए नीति	❖ संवेदनशील वैयक्तिक डेटा या सूचना सहित वैयक्तिक सूचना को संभालने या व्यवहार करने के लिए एक गोपनीयता नीति उपलब्ध कराना। उक्त नीति निम्नलिखित के लिए व्यवस्था करेगीः • उसके व्यवहारों और नीतियों के स्पष्ट और आसानी से पहुँच-योग्य विवरण; • संगृहीत वैयक्तिक या संवेदनशील वैयक्तिक डेटा या सूचना का प्रकार; • ऐसी सूचना के संग्रहण और उपयोग का प्रयोजन; • संवेदनशील वैयक्तिक डेटा या सूचना सहित सूचना का प्रकटीकरण; • उचित सुरक्षा प्रथाएँ और प्रक्रियाएँ; • नीति वेबसाइट पर प्रकाशित की जाएगी।
सूचना का संग्रहण	❖ संग्रहण के लिए सहमति लिखित में प्राप्त की जानी चाहिए। इस प्रकार संगृहीत सूचना केवल निम्नलिखित के लिए होनी चाहिए • एक विधिसम्मत प्रयोजन के लिए, • आवश्यक समझे जाने पर तथा • निगमित निकाय या उसकी ओर से किसी व्यक्ति के किसी कार्य या गतिविधि से संबद्ध रूप में। ❖ साथ ही, सूचना के प्रदाता के पास निम्नलिखित का होना आवश्यक है • इस तथ्य की जानकारी कि सूचना का संग्रहण किया जा रहा है,

	• वह प्रयोजन जिसके लिए सूचना का संग्रहण किया जा रहा है, • सूचना के उद्दिष्ट प्राप्तकर्ता, • उस एजेंसी का नाम और पता जो सूचना का संग्रहण कर रही है, तथा • वह एजेंसी जो सूचना का प्रतिधारण करेगी। ❖ इस प्रकार प्रदान की गई सूचना को यदि गलत अथवा अपूर्ण पाया जाता है तो सूचना के प्रदाता को उसमें सुधार / संशोधन करने की अनुमति दी जानी चाहिए। ❖ सूचना के प्रदाता के पास एक विकल्प है- • संग्रहण के लिए अपेक्षित डेटा अथवा सूचना प्रदान न करने का विकल्प, • पहले दिये गये अपनी सहमति को वापस लेने का विकल्प • सहमति को इस प्रकार वापस लेने की बात निगमित निकाय को लिखित में भेजी जाएगी ❖ सूचना उन प्रयोजनों के लिए अपेक्षित समय से अधिक नहीं रखी जाएगी जिनके लिए सूचना का उपयोग विधिसम्मत रूप में किया जाएगा तथा फिलहाल प्रचलित किसी अन्य विधि के अंतर्गत अन्यथा अपेक्षित समय से अधिक नहीं रखी जाएगी।
सूचना का प्रकटीकरण	❖ किसी अन्य पक्षकार को प्रकटीकरण की स्थिति में सूचना के प्रदाता से अनिवार्यतः पूर्व अनुमति संविदा के रूप में अथवा इसके प्रकटीकरण के लिए विशिष्ट रूप से अन्य प्रकार से प्राप्त की जाएगी। ❖ ऐसी सहमति सरकारी एजेंसियों के साथ साझा करने की स्थिति में अथवा जहाँ ऐसा प्रकटीकरण किसी विधिक दायित्व के अनुपालन के लिए आवश्यक है, आवश्यक नहीं होगी।
सूचना का अंतरण	❖ अंतरण करते समय निम्नलिखित शर्तें पूरी की जानी चाहिएः • जिस स्तर के डेटा संरक्षण का पालन निगमित निकाय (अंतरणकर्ता) द्वारा किया जाता है, उसी स्तर का पालन प्राप्त करनेवाले पक्षकार

	(अंतरिती) के द्वारा किया जाएगा। • निगमित निकाय अथवा उसकी ओर से किसी व्यक्ति और सूचना के प्रदाता के बीच विधिसम्मत संविदा का निष्पादन आवश्यक है। • ऐसे व्यक्ति ने डेटा के अंतरण के लिए सहमति दी है।
शिकायत प्रबंध	❖ निगमित निकाय एक शिकायत अधिकारी को पदनामित करे ❖ उसके नाम और संपर्क का विवरण अपनी वेबसाइट पर प्रकाशित करे ❖ शिकायतों का समाधान एक महीने के अंदर किया जाए।
युक्तिसंगत सुरक्षा व्यवहार और क्रियाविधियाँ	❖ सुरक्षा व्यवहारों और मानकों का कार्यान्वयन किया जाए • आईएस/आईएसओ/आईईसी 27001 • सूचना सुरक्षा कार्यक्रम के रूप में व्यवहारों और मानकों का प्रलेखीकरण जिसमें निम्नलिखित निहित हों ○ प्रबंधकीय, ○ तकनीकी, ○ परिचालनगत और भौतिक सुरक्षा नियंत्रण उपाय ❖ डेटा संरक्षण के लिए सर्वोत्तम व्यवहारों के कूट (किसी उद्योग संघ या ऐसे संघ द्वारा बनाई गई किसी संस्था के द्वारा, जिनके सदस्य सर्वोत्तम व्यवहारों के आईएस/ आईएसओ/ आईईसी कूटों को छोड़कर अन्य कूटों का अनुसरण करने के द्वारा स्व-विनियमन कर रहे हों) ❖ ऐसे मानक या सर्वोत्तम व्यवहारों के कूट कम से कम वर्ष में एक बार, अथवा जब भी उसकी प्रक्रिया और कंप्यूटर संसाधन के उल्लेखनीय कोटि-उन्नयन किया जाता है तब केन्द्र सरकार द्वारा विधिवत् अनुमोदित स्वतंत्र संपरीक्षक के माध्यम से प्रमाणित अथवा संपरीक्षित किये जाने चाहिए।

आईटी सेवा प्रदाता (आईटी मध्यवर्ती) का दायित्व

यह सुनिश्चित करने के लिए कि सूचना को संभालने और प्रसंस्करण करनेवाले मध्यवर्ती को दायित्व के संबंध में संरक्षित रखा जाए, वे अन्य पक्षकार की सूचना को संभालते समय पर्याप्त उचित सावधानी सुनिश्चिक करेंगे। आईटी अधिनियम, 2000 की धारा 79 इंटरनेट सेवा प्रदाताओं सहित बीमा मध्यवर्तियों के दायित्व के लिए व्यवस्था करती है। आईटी अधिनियम की धारा 79 का संशोधन आईटी (संशोधन) अधिनियम, 2008 के द्वारा किया गया। उपर्युक्त संशोधन के अनुसरण में कोई भी मध्यवर्ती उनके द्वारा उपलब्ध कराये गये अथवा मेजबानी किये गये किसी अन्य पक्षकार के सूचना, डेटा अथवा संचार लिंक के लिए जिम्मेदार नहीं होगा, यदिः

- मध्यवर्ती का कार्य एक संचार प्रणाली को प्रवेश देने तक सीमित है जिस पर अन्य पक्षकारों के द्वारा उपलब्ध कराई गई सूचना प्रेषित की गई है अथवा अस्थायी तौर पर रखी गई है;
- मध्यवर्ती प्रेषण को प्रारंभ नहीं करता अथवा प्रेषण के प्राप्तकर्ता का चयन नहीं करता, तथा प्रेषण में निहित सूचना का चयन अथवा आशोधन नहीं करता;
- मध्यवर्ती अपने कर्तव्यों का निर्वहण करते समय समुचित सावधानी बरतता है तथा इस संबंध में केन्द्र सरकार द्वारा निर्धारित किये जानेवाले ऐसे अन्य दिशानिर्देशों का पालन भी करता है।

यह ध्यान रखा जाए कि मध्यवर्ती उपर्युक्त उन्मुक्ति खो देगा यदि मध्यवर्ती के संबंध में यह पाया जाता है कि उसने षडयंत्र किया है अथवा अवप्रेरित किया है अथवा सहायता दी है अथवा प्रलोभन दिया है चाहे अवैध कार्य के आचरण में धमकियों के द्वारा हो या वचन देने के द्वारा या अन्य प्रकार से। इसके अलावा, यदि मध्यवर्ती वास्तविक ज्ञान प्राप्त करने पर, अथवा यह सूचित किये जाने पर कि मध्यवर्ती के द्वारा नियंत्रित कंप्यूटर संसाधन में स्थित अथवा उसके साथ संबद्ध कोई भी सूचना, डेटा अथवा संचार लिंक का उपयोग अवैध कार्य़ करने के लिए किया जा रहा है, मध्यवर्ती किसी भी प्रकार से साक्ष्य को निष्प्रभावी किये बिना उस संसाधन पर विद्यमान सामग्री तक पहुँच को शीघ्रतापूर्वक नहीं हटाता अथवा अशक्त नहीं करता।

सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश) नियम, 2011

केन्द्र सरकार ने अतिरिक्त रूप से अधिसूचना दिनांक 11 अप्रैल 2011 के अनुसार सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश) नियम, 2011 अधिसूचित किये हैं। ये नियम मध्यवर्तियों द्वारा समुचित सावधानी तथा लिपिबद्धीकरण के प्रबंध और प्रक्रियागत दायित्वों के भाग के रूप में मध्यवर्तियों द्वारा व्यवहार किये जानेवाले दिशानिर्देश और क्रियाविधि उपलब्ध कराते हैं।

मध्यवर्ती द्वारा बरती जानेवाली समुचित सावधानी	**कार्रवाई योग्य बातें**
नियम और विनियम, गोपनीयता नीति तथा प्रवेश - अथवा किसी भी व्यक्ति के द्वारा मध्यवर्ती के कंप्यूटर संसाधन का उपयोग करने के लिए प्रयोक्ता करार प्रकाशित करना	ऐसे नियम और विनियम, निबंधन और शर्तें अथवा प्रयोक्ता करार, कंप्यूटर संसाधन के प्रयोक्ताओं को सूचित करेंगे कि वे ऐसी किसी सूचना की मेजबानी, प्रदर्शन, अपलोडिंग, आशोधन, प्रकाशन, प्रेषण, अद्यतनीकरण अथवा साझेदारी न करें जो • किसी अन्य व्यक्ति के स्वामित्व में है और जिसके लिए प्रयोक्ता के पास कोई अधिकार नहीं है; • समग्र रूप में हानिकारक, उत्पीड़क, ईशनिंदात्मक, मानहानिकारक, अभद्र, अश्लील, बालयौनआकर्षक, अपमानजनक, अन्य व्यक्तियों की गोपनीयता के प्रति आक्रामक, घृणित, अथवा प्रजातीय तौर पर, नृजातीय रूप से आपत्तिजनक, निंदक, धन-शोधन या जूए का प्रोत्साहक अथवा किसी भी अन्य प्रकार से अवैध है; • किसी भी प्रकार से अवयस्कों के लिए हानि पहुँचाती है; • किसी एकस्व (पेटेंट), व्यापार-चिह्न (ट्रेडमार्क), प्रतिलिप्यधिकार (कापीराइट) अथवा अन्य स्वामित्व संबंधी अधिकारों का उल्लंघन करती है; • फिलहाल प्रचलन में स्थित किसी कानून का उल्लंघन करती है; • ऐसे संदेशों के स्रोत के बारे में पानेवाले को धोखा देती है या भ्रमित करती है अथवा ऐसी कोई सूचना संप्रेषित करती है जो कुल मिलाकर घृणास्पद या धमकाने के स्वरूप की है; • किसी अन्य व्यक्ति का छद्म रूप धारण करती

	है; • किसी कंप्यूटर संसाधन की कार्यात्मकता को अवरुद्ध, नष्ट अथवा सीमित करने के लिए अभिकल्पित साफ्टवेयर विषाणुओं या किसी अन्य कंप्यूटर कोड, फाइलों अथवा प्रोग्रामों से युक्त है; • भारत की एकता, अखंडता, रक्षा, सुरक्षा अथवा प्रभुसत्ता, विदेशी राज्यों के साथ मैत्रीपूर्ण संबंधों, अथवा सार्वजनिक सुव्यवस्था को जोखिम में डालती है अथवा किसी संज्ञेय अपराध के कृत्य के लिए प्रेरणा का कारण बनती है अथवा किसी अपराध की जाँच को रोकती है अथवा किसी अन्य राष्ट्र का अपमान करती है।
मेजबानी (होस्टिंग)/प्रेषण संबंधी दायित्व	मध्यवर्ती `जानबूझकर' किसी सूचना की मेजबानी नहीं करेगा या उसे प्रकाशित नहीं करेगा या *उसका प्रेषण प्रारंभ नहीं करेगा,* प्रेषण के प्राप्तकर्ता का चयन नहीं करेगा. तथा प्रेषण में निहित सूचना का चयन नहीं करेगा या उसका आशोधन नहीं करेगा।
लिपिबद्धीकरण (टेक डाउन) का दायित्व	मध्यवर्ती से अपेक्षित है कि वह जानकारी मिलने से 36 घंटों के अंदर ऐसी सूचना को निर्योग्य बनायेगा जो उपर्युक्त का उल्लंघन करता है। मध्यवर्ती ऐसी सूचना और संबद्ध अभिलेखों का परिरक्षण भी जाँच के प्रयोजनों के लिए कम से कम नब्बे दिन के लिए करेगा।
समापन का अधिकार	नियमों और विनियमों, प्रयोक्ता करार और गोपनीयता नीति का अनुपालन न करने की स्थिति में मध्यवर्ती के कंप्यूटर संसाधन के प्रयोक्ताओं के प्रवेश अथवा उपयोग को तत्काल समाप्त करने का अधिकार मध्यवर्ती के पास होगा।
सूचित करने का दायित्व	मध्यवर्ती से अपेक्षित होगा कि वह भारतीय कंप्यूटर आपात स्थिति प्रतिक्रिया टीम को साइबर सुरक्षा संबंधी घटनाओं की सूचना दे और साथ ही, साइबर सुरक्षा घटनाओं से संबंधित सूचना का साझा उक्त टीम से करे।
सूचना प्रदान करने का दायित्व	मध्यवर्ती जाँच-पड़ताल संबंधी, संरक्षण संबंधी, साइबर सुरक्षा कार्यकलाप के लिए सरकारी एजेंसियों को सूचना प्रदान करेगा अथवा सहायता देगा।

युक्तिसंगत उपाय	मध्यवर्ती से समय-समय पर अपेक्षित है कि उसके पास अपने कंप्यूटर संसाधन और उसमें निहित सूचना की सुरक्षा के लिए सूचना प्रौद्योगिकी (युक्तिसंगत सुरक्षा प्रथाएँ और प्रक्रियाएँ तथा संवेदनशील वैयक्तिक सूचना) नियम, 2011 में निर्धारित रूप में युक्तिसंगत सुरक्षा प्रथाओं और प्रक्रियाओं का अनुसरण करते हुए सभी उपाय हों।
शिकायत अधिकारी	मध्यवर्ती से अपेक्षित है कि वह एक शिकायत अधिकारी की नियुक्ति करे तथा उसके संपर्क का विवरण एवं व्यवस्था का ब्योरा उपलब्ध हो जिसके द्वारा कोई भी पीड़ित व्यक्ति अपनी शिकायतें सूचित कर सके। उक्त शिकायत अधिकारी शिकायत की प्राप्ति की तारीख से एक महीने के अंदर शिकायतों का समाधान करेगा।

भारतीय कंप्यूटर आपाती प्रतिक्रिया टीम

भारत सरकार ने सूचना प्रौद्योगिकी (भारतीय कंप्यूटर आपाती प्रतिक्रिया टीम तथा कार्य और कर्तव्य निष्पादित करने की पद्धति) नियम, 2013 अधिसूचित किये हैं।

आईटी (भारतीय कंप्यूटर आपाती प्रतिक्रिया टीम तथा कार्य और कर्तव्य निष्पादित करने की पद्धति) नियम, 2013 के नियम 12(1)(क) के अनुसार, साइबर सुरक्षा घटनाओं से प्रभावित कोई भी व्यक्ति, संगठन अथवा कारपोरेट संस्था घटना की सूचना सर्ट-इन, सेवा प्रदाताओं, मध्यवर्तियों, डेटा केन्द्रों क़ो दे तथा निगमित निकाय साइबर सुरक्षा घटनाओं के संबंध में समय पर कार्रवाई करने के लिए घटना के घटित होने की सूचना घटना की जानकारी मिलने पर एक उचित समय के अंदर कार्रवाई करने की गुंजाइश रखते हुए सर्ट-इन को देगा।

निम्नलिखित प्रकार की साइबर सुरक्षा घटनाएँ अधिदेशात्मक (मैंडेटरी) तौर पर कार्रवाई करने की गुंजाइश रखते हुए यथाशीघ्र सर्ट-इन को सूचित की जाएँगी।

- संकटपूर्ण नेटवर्कों / प्रणालियों का लक्ष्यीकृत स्कैनिंग / अन्वेषण
- संकटपूर्ण प्रणालियों / सूचना का समाधान
- आईटी प्रणालियों / डेटा तक अनधिकृत प्रवेश
- वेबसाइट का विरूपण अथवा वेबसाइट में घुसपैठ और अनधिकृत परिवर्तन जैसे दुर्भावपूर्ण कूट, बाहरी वेबसाइटों के साथ लिंक आदि

- दुर्भावपूर्ण कूट आक्रमण जैसे विषाणु (वाइरस)/कीड़ा (वर्म)/साहसिक (त्रोज़न)/बाटनेट्स/ स्पाईवेयर
- सर्वरों पर आक्रमण जैसे डेटाबेस, मेल और डीएनएस तथा नेटवर्क साधन जैसे रूटर।
- पहचान की चोरी, धोखा देना (स्पूफ़िंग) और फिशिंग आक्रमण
- सेवा का अस्वीकरण (डीओएस) और वितरित सेवा के अस्वीकरण (डीडीओएस) आक्रमण
- महत्वपूर्ण बुनियादी व्यवस्था, एससीएडीए प्रणालियों और बेतार (वायरलेस) नेटवर्कों पर आक्रमण
- अनुप्रयोगों, जैसे ई-गवर्नैंस, ई-कामर्स आदि पर आक्रमण।

डेटा चोरी

डेटा चोरी से प्रतिलिप्यधिकार (कापीराइट) उल्लंघन, आईटी अधिनियम 2000 के अधीन गोपनीयता का उल्लंघन, एवं भारतीय दंड संहिता, 1860 के अधीन आपराधिक विश्वासघात और कपटपूर्ण दुरुपयोग के विषय संबद्ध हैं।

सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 66 के साथ पठित धारा 43(ख) तथा भारतीय दंड संहिता की धारा 379, 405 और 420 डेटा चोरी और उसके दंडात्मक प्रावधानों की रूपरेखा से संबंधित हैं।

कंप्यूटर, कंप्यूटर प्रणाली की क्षति के लिए अर्थदंड और क्षतिपूर्ति

धारा 43 स्पष्ट रूप से उस व्यक्ति के विरुद्ध क्षतिपूर्ति के रूप में हर्जाने के उपबंधों के लिए व्यवस्था करती है जो कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क के स्वामी अथवा प्रभारी की अनुमति के बिना

(क) ऐसे कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क अथवा कंप्यूटर संसाधन में प्रवेश करता है अथवा प्रवेश प्राप्त करता है;

(ख) किसी अलग करने योग्य भंडारण माध्यम में धारित या भंडारण की गई सूचना या डेटा सहित, ऐसे कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क से कोई भी डेटा, कंप्यूटर डेटा बेस या सूचना को डाउनलोड करता है, उसकी प्रतिलिपि बनाता है अथवा उसे उद्धृत करता है;

(ग) किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में कोई कंप्यूटर संदूषक या कंप्यूटर विषाणु (वाइरस) प्रविष्ट करता है अथवा प्रविष्ट करवाता है;

(घ) ऐसे कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क में स्थित किसी कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क, डेटा, कंप्यूटर डेटा बेस अथवा किन्हीं अन्य प्रोग्रामों को क्षतिग्रस्त करता है अथवा क्षतिग्रस्त करवाता है;

(ङ) किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क को विघटित करता है अथवा विघटित करवाता है;

(च) किसी भी प्रकार से किसी कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क में प्रवेश करने के लिए अधिकृत किसी व्यक्ति को प्रवेश देने से इनकार करता है अथवा इनकार करवाता है;

(छ) इस अधिनियम, उसके अधीन बनाये गये नियमों अथवा विनियमों के उपबंधों का उल्लंघन करते हुए किसी कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क में प्रवेश को सुसाध्य बनाने के लिए किसी व्यक्ति को कोई सहायता उपलब्ध कराता है;

(ज) किसी कंप्यूटर, कंप्यूटर प्रणाली, अथवा कंप्यूटर नेटवर्क में हेरफेर करते हुए अथवा छल-कपट करते हुए किसी एक व्यक्ति के द्वारा उपयोग की गई सेवाओं के लिए किसी अन्य व्यक्ति के खाते में प्रभार वसूल करता है;

(झ) किसी भी प्रकार से किसी कंप्यूटर संसाधन में स्थित किसी सूचना को नष्ट करता है, उसका विलोपन करता है अथवा उसमें परिवर्तन करता है अथवा उसके मूल्य या उपयोग में कमी करता है अथवा हानिकर ढंग से उसे प्रभावित करता है;

(ञ) क्षति पहुँचाने के उद्देश्य से किसी कंप्यूटर संसाधन के लिए प्रयुक्त किसी कंप्यूटर स्रोत कूट की चोरी करता है, छिपाता है, नष्ट करता है अथवा उसमें परिवर्तन करता है अथवा किसी व्यक्ति से उसकी चोरी करवाता है, उसे छिपवाता है, नष्ट करवाता है अथवा उसमें परिवर्तन करवाता है।

गोपनीयता और गुप्तता

धारा 72क ऐसे इलेक्ट्रानिक अभिलेखों अथवा सूचना की गोपनीयता और गुप्तता को सुनिश्चित करने के दायित्व की व्यवस्था करती है जिसके लिए किसी भी व्यक्ति ने प्रवेश की अनुमति प्राप्त की है। ऐसी किसी सूचना/ अभिलेख का प्रकटीकरण संबंधित व्यक्ति की सहमति के बिना किसी अन्य व्यक्ति को नहीं किया जा सकता। गोपनीयता और गुप्तता को बनाये न रखना व्यक्ति को दंड का भागी बनाता है।

इसी प्रकार, धारा 72क मध्यवर्ती सहित किसी ऐसे व्यक्ति के लिए भी दायित्व की व्यवस्था करती है जिसने सेवाएँ प्रदान करते समय किसी अन्य व्यक्ति के बारे में वैयक्तिक सूचना से निहित किसी सामग्री तक विधिसम्मत संविदा की शर्तों के अंतर्गत

प्रवेश की अनुमति प्राप्त की हो, यदि संबंधित व्यक्ति की सहमति के बिना अथवा विधिसम्मत संविदा का उल्लंघन करते हुए प्रकटीकरण करता है, तो वहाँ ऐसा व्यक्ति दंड का भागी होगा।

दंड संबंधी उपबंध

निम्नलिखित चार्ट में उल्लंघनों के परिणामों से संबंधित सूचना प्रौद्योगिकी अधिनियम, 2000 के अंतर्गत यथाप्रयोज्य दंड संबंधी उपबंधों का सारांश दिया गया है

न्यायनिर्णयन अधिकारी

धारा 46 के अनुसार, केन्द्र सरकार / राज्य सरकार यह निर्णय करने के लिए कि क्या किसी व्यक्ति ने अधिनियम अथवा अधिनियम के अंतर्गत विद्यमान किसी नियम, निदेश या आदेश का कोई उल्लंघन किया है, शक्ति के साथ उक्त विषय में जाँच आयोजित करने के लिए न्यायनिर्णयन अधिकारी के रूप में एक निदेशक से अन्यून दरजे के अधिकारी की नियुक्ति कर सकती है। आर्थिक क्षेत्राधिकार रु. 5 करोड़ है।

साइबर अपीलीय न्यायाधिकरण

सरकार ने साइबर अपीलीय न्यायाधिकरण (सीएटी) का गठन किया है जिन्हें न्यायनिर्णयन अधिकारी (एओ) के निर्णयों के संबंध में अपील प्रस्तुत की जा सकती है। सीएटी के निर्णय के विरुद्ध अपील उच्च न्यायालय में प्रस्तुत की जा सकती है।

दंड संबंधी उपबंध

निम्नलिखित चार्ट में सूचना प्रौद्योगिकी अधिनियम, 2000 के अंतर्गत यथाप्रयोज्य दंड संबंधी उपबंधों का सारांश दिया गया है जो उल्लंघनों के परिणामों से संबंधित हैं

धारा	**दंड**
43क (डेटा का संरक्षण न करना)	इस प्रकार प्रभावित व्यक्ति को क्षतिपूर्ति के रूप में हर्जाना • रु. 5 करोड़ तक (न्यायनिर्णयन अधिकारी) • रु. 5 करोड़ से अधिक (सिविल न्यायालय)

65 (सूचना-तस्करी (हैकिंग)/ हेर-फेर करना (टैम्परिंग)	तीन वर्ष तक विस्तारयोग्य कारावास, अथवा अर्थदंड सहित जो दो लाख रुपये तक हो सकता है, अथवा दोनों।
66 (कंप्यूटर संबंधी अपराध)	तीन वर्ष की अवधि तक विस्तारणीय कारावास अथवा पाँच लाख तक विस्तारणीय अर्थदंड अथवा दोनों
66ख (चोरी किये गये कंप्यूटर संसाधन को बेईमानी से प्राप्त करना)	तीन वर्ष तक विस्तारणीय कारावास अथवा एक लाख रुपये तक विस्तारणीय अर्थदंड अथवा दोनों के साथ दंडनीय
66ग (पहचान की चोरी)	तीन वर्ष तक विस्तारणीय कारावास और अर्थदंड से भी दंडनीय जो एक लाख तक विस्तारणीय है।
66ङ (गुप्तता के उल्लंघन के लिए दंड)	तीन वर्ष तक विस्तारणीय कारावास अथवा दो लाख रुपये से अनधिक अर्थदंड के साथ, अथवा दोनों के साथ
66च (साइबर आतंकवाद)	आजीवन कारावास
67ग (मध्यवर्तियों द्वारा सूचना का परिरक्षण और प्रतिधारण)	तीन वर्ष तक की अवधि के लिए विस्तारणीय कारावास और अर्थदंड से भी दंडनीय।
71 (नियंत्रक अथवा प्रमाणकर्ता प्राधिकारी के पास महत्वपूर्ण तथ्य की गलतबयानी)	दो वर्ष तक विस्तारणीय अवधि के लिए कारावास अथवा रु. 1 लाख तक विस्तारणीय अर्थदंड अथवा दोनों के साथ
72 (गोपनीयता और गुप्तता का भंग)	2 वर्ष तक विस्तारणीय अवधि के लिए कारावास, अथवा एक लाख रुपये तक विस्तारणीय अर्थदंड अथवा दोनों के साथ।
72क (विधिसम्मत संविदा का उल्लंघन करते हुए सूचना का प्रकटीकरण)	3 वर्ष तक विस्तारणीय अवधि के लिए कारावास अथवा अर्थदंड जो पाँच लाख रुपये तक विस्तारणीय है, अथवा दोनों के साथ
73 (झूठा इलेक्ट्रानिक हस्ताक्षर प्रमाणपत्र प्रकाशित करना)	दो वर्ष तक विस्तारणीय अवधि के लिए कारावास, अथवा एक लाख रुपये तक विस्तारणीय अर्थदंड, अथवा दोनों के साथ दंडनीय।
74 (कपटपूर्ण प्रयोजन के लिए प्रकाशन)	दो वर्ष तक की विस्तारणीय अवधि के लिए कारावास, अथवा एक लाख रुपये तक विस्तारणीय अर्थदंड, अथवा दोनों के साथ
85 (कंपनियों द्वारा अपराध)	प्रत्येक व्यक्ति जो उल्लंघन घटित होते समय

	प्रभारी रहा हो, उल्लंघन के लिए दोषी होगा। जहाँ उल्लंघन किसी कंपनी द्वारा किया गया है और यह प्रमाणित होता है कि उक्त उल्लंघन कंपनी के किसी निदेशक, प्रबंधक, सचिव अथवा अन्य अधिकारी की सहमति अथवा मिलीभगत से घटित हुआ है, वहाँ ऐसे निदेशक, प्रबंधक, सचिव अथवा अन्य अधिकारी को भी उक्त उल्लंघन का दोषी माना जाएगा।

अधिनियम/ संविधि	**अपेक्षा**	
सूचना प्रौद्योगिकी अधिनियम, 2000 (इलेक्ट्रानिक अभिलेखों और इलेक्ट्रानिक हस्ताक्षर के लिए ई-गवर्नेंस ढाँचा)	• इलेक्ट्रानिक अभिलेखों और इलेक्ट्रानिक हस्ताक्षर का अधिप्रमाणन (धारा 3 और 3क)	• इलेक्ट्रानिक अभिलेखों का अधिप्रमाणन डिजिटल हस्ताक्षर के माध्यम से किया जाना चाहिए जिस स्थिति में वह विषम गुप्त प्रणाली का उपयोग करते हुए तथा एक निजी कुंजी और एक सरकारी कुंजी के साथ पीकेआई बुनियादी व्यवस्था का उपयोग करते हुए हैश कार्य के द्वारा होना चाहिए। इसमें आवश्यक रूप से इलेक्ट्रानिक हस्ताक्षर के लिए डीएससी का उपयोग शामिल किया जाना चाहिए। • इलेक्ट्रानिक अभिलेख का एक अधिप्रमाणन ऐसी तकनीक का उपयोग करते हुए भी किया जा सकता है जो विश्वसनीय हो और अधिनियम की दूसरी अनुसूची में विनिर्दिष्ट रूप में हो।
	• इलेक्ट्रानिक अभिलेख और इलेक्ट्रानिक हस्ताक्षर की विधिक मान्यता (धारा 4 और 5)	• जब भी विधि द्वारा लिखित में किसी सूचना की अपेक्षा की जाती है, तब ऐसी अपेक्षा पूरी की जाने के तौर पर समझी जाएगी यदि उक्त सूचना इलेक्ट्रानिक रूप में दी जाती है अथवा उपलब्ध कराई जाती है तथा वह पहुँच-

		योग्य है जिससे उसका उपयोग किसी परवर्ती संदर्भ के लिए किया जा सके। • जब भी कोई विधि किसी सूचना के संबंध में अपेक्षा करती है कि उसपर किसी व्यक्ति के द्वारा हस्ताक्षर किये जाएँ, तब ऐसी अपेक्षा पूरी किये जाने के रूप में तब समझी जाएगी यदि उस पर इलेक्ट्रानिक रूप से हस्ताक्षर किये जाएँ।
	• इलेक्ट्रानिक अभिलेख का प्रतिधारण और दस्तावेजों का संपरीक्षण (धारा 7 और 7क)	• इलेक्ट्रानिक अभिलेखों का प्रतिधारण इलेक्ट्रानिक तौर पर किया जा सकता है जब कोई विधि अपेक्षा करती है कि किसी दस्तावेज या सूचना का प्रतिधारण एक विनिर्दिष्ट अवधि के लिए किया जाए। तथापि, इलेक्ट्रानिक रूप में परिरक्षित दस्तावेज के संपरीक्षण के संबंध में प्रतिधारण के लिए कोई अवधि विनिर्दिष्ट नहीं की गई है।
	• इलेक्ट्रानिक साधनों के द्वारा संविदाओं की विधिमान्यता (धारा 10क)	• इलेक्ट्रानिक रूप में प्रस्तावों और स्वीकृति के द्वारा स्थापित संविदा प्रवर्तनीय है।
	• इलेक्ट्रानिक अभिलेखों का अधिकार, इवेक्ट्रानिक अभिलेखों की स्वीकृति तथा प्रेषण का समय और स्थान (धारा 11, 12 और 13)	• इलेक्ट्रानिक अभिलेख प्रवर्तक का माना जाता है यदि वह प्रवर्तक द्वारा अथवा प्राधिकृत व्यक्ति द्वारा अथवा सूचना प्रणाली द्वारा भेजा गया हो। • प्राप्ति-स्वीकृति विनिर्दिष्ट रूप या पद्धति में प्रवर्तक द्वारा की जाती है। • इलेक्ट्रानिक अभिलेख ऐसे समय प्रेषित किया जाता है जब वह प्रवर्तक के नियंत्रण के बाहर कंप्यूटर संसाधन में प्रवेश करता है।

		• प्राप्ति का समय इस सिद्धांत पर आधारित होगा - प्राप्ति तब घटित होती है जब इलेक्ट्रानिक अभिलेख उद्दिष्ट कंप्यूटर में प्रवेश करता है यदि विनिर्दिष्ट किया गया है। अन्य मामलों में, प्राप्ति ऐसे समय घटित होती है जब इलेक्ट्रानिक अभिलेख पानेवाले के द्वारा पुनः प्राप्त किया जाता है।
	• इलेक्ट्रानिक अभिलेख, इलेक्ट्रानिक हस्ताक्षर और सुरक्षा प्रक्रिया प्राप्त करना (धारा 14, 15 और 16)	• इलेक्ट्रानिक अभिलेख के संबंध में सुरक्षा प्रक्रिया का उपयोग किया जाना चाहिए और तब ऐसे इलेक्ट्रानिक अभिलेख को सुरक्षित माना जाएगा।
सूचना प्रौद्योगिकी अधिनियम, 2000 (दंड, क्षतिपूर्ति और अपराध)	• अनधिकृत प्रवेश के कारण कंप्यूटर और कंप्यूटर प्रणाली को क्षति (धारा 43) • डेटा क्षतिपूर्ति का संरक्षण न करना (धारा 43क) • साइबर अपराध से संबंधित अपराध (धारा 65, 66, 67) • गोपनीयता और गुप्तता का उल्लंघन (धारा 72) • सूचना के प्रकटीकरण और	ऊपर सम्मिलित किया गया है

	विधिमान्य संविदा के उल्लंघन के लिए दंड (धारा 72क) • कंपनियों द्वारा अपराध (धारा 85)	

अधिनियम / संविधि	**अपेक्षा**	
सूचना प्रौद्योगिकी (युक्तिसंगत सुरक्षा व्यवहार और प्रक्रिया तथा संवेदनशील वैयक्तिक डेटा या सूचना)	• संवेदनशील वैयक्तिक डेटा और सूचना के संग्रहण, अंतरण, भंडारण, प्रकटीकरण तथा प्रसंस्करण के लिए प्रक्रिया • युक्तिसंगत सुरक्षा व्यवहारों और सर्वोत्तम प्रथाओं का कार्यान्वयन • वर्ष में एक बार स्वतंत्र संपरीक्षक द्वारा नियमित आधार पर प्रमाणीकरण/ संपरीक्षण	ऊपर सम्मिलित किया गया है।
सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश) नियम, 2011	• मध्यवर्ती द्वारा समुचित सावधानी और उनका दायित्व • मध्यवर्ती द्वारा युक्तसंगत सुरक्षा	• ऊपर सम्मिलित किया गया है

	व्यवहारों का कार्यान्वयन • आईसीईआरटी को साइबर सुरक्षा संबंधी घटना की सूचना देना	
सूचना प्रौद्योगिकी (सुरक्षा प्रक्रिया) नियम, 2004	• एक सुरक्षित डिजिटल हस्ताक्षर बनाने के लिए पूरी की जानेवाली अपेक्षाएँ	• सुरक्षित डिजिटल हस्ताक्षर के द्वारा सुरक्षित इलेक्ट्रानिक अभिलेखों के अधिप्रमाणन के लिए नियम • सरकारी कुंजी / निजी कुंजी / स्मार्ट कार्ड
सूचना प्रौद्योगिकी (सूचना के अवरोधन, निगरानी के लिए प्रक्रिया और रक्षोपाय) नियम, 2009	• सूचना का अवरोधन और कूटलेखन का सामान्य भाषा में परिवर्तन	• कंप्यूटर संसाधनों में उत्पन्न, प्रेषित, प्राप्त अथवा संचित सूचना के अवरोधन, निगरानी अथवा कूटलेखन को खोलने के लिए सरकारी एजेंसी को प्राधिकृत करना
वेबसाइट को अवरुद्ध करने के लिए प्रक्रिया	• सरकारी अधिसूचना दिनांक 27 फरवरी 2003, जी.एस.आर. 18(ई)	• वेबसाइटों को अवरुद्ध करने के संदर्भ में अनुदेश देने के लिए इंडिया (सर्ट-इंड) एकल प्राधिकरण है।
टेलीकाम अनपेक्षित वाणिज्यिक संचार विनियम, 2007 और टेलीकाम वाणिज्यिक संचार ग्राहक अधिमान विनियम, 2010	• अनपेक्षित वाणिज्यिक संचार के साथ व्यवहार करने के लिए प्रक्रिया तथा प्रवेश प्रदाताओं और दूरस्थ विपणनकर्ताओं के दायित्व	• डीएनडी के अंतर्गत पंजीकृत संख्याओं के लिए गुप्तता • जिन्होंने अनिच्छा का विकल्प दिया है उनके लिए कोई काल या एसएमएस संभव नहीं है • दूरस्थ विपणन के लिए केवल 140 शृंखला संख्या का ही प्रयोग करना होगा।

क्षेत्र के नाम में विवाद समाधान नीति और प्रक्रिया (आईएनडीआरपी)	• पंजीयक और शिकायतकर्ता के बीच इंटरनेट क्षेत्र नामों में विवादों से संबंधित प्रक्रिया	• विवादों के प्रकार लाये जा सकते हैं, तथा मानदंडों के विषय में विवाचकों द्वारा विचार किया जाएगा। • प्रक्रिया के आईएनडीआरपी नियम। इन नियमों में यह वर्णन है कि एक शिकायत कैसे फाइल करनी चाहिए, एक शिकायत की प्रतिक्रया कैसे करनी चाहिए, शुल्क, संचार और प्रयुक्त की जानेवाली अन्य प्रक्रियाएँ।

अधिनियम/ संविधि	**अपेक्षा**	
बीमा अधिनियम	• ई-बीमा पालिसियों के निर्गम संबंधी विनियमन • बीमा अभिलेख के अनुरक्षण संबंधी विनियमन	• इलेक्ट्रानिक रूप में पालिसियों के निर्गम और साथ ही, ई-रूप में दावा अभिलेखों सहित बीमा अभिलेख अनुरक्षित करने के लिए नीति के लिए दिशानिर्देश। • ई-पालिसियों के निर्गम के लिए ईआईए का अनुरक्षण किया जाना चाहिए।
केन्द्रीय केवाईसी अभिलेख रजिस्ट्री	• ग्राहकों की केवाईसी की इलेक्ट्रानिक प्रति फाइल करना	• केन्द्रीय केवाईसी के माध्यम से केन्द्रीय केवाईसी को समर्थ बनाना • केन्द्रीय केवाईसी में अपलोड की जानेवाली इलेक्ट्रानिक प्रति
भारतीय साक्ष्य अधिनियम, 1872	• इलेक्ट्रानिक अभिलेखों का स्वीकरण	• साक्ष्य के रूप में स्वीकृत इलेक्ट्रानिक अभिलेख (धारा 3) • धारा 65ए और 65बी इलेक्ट्रानिक साक्ष्य देने के लिए प्रक्रियाएँ और मानक (आईटी अधिनियम, 2000 के अनुसार सिद्ध की जानेवाली अभिलेखों की प्रामाणिकता) उपलब्ध कराती हैं। • धारा 85ए, 85बी, 85सी और 88ए इलेक्ट्रानिक करारों, इलेक्ट्रानिक

		अभिलेखों तथा डिजिटल हस्ताक्षरों/ डिजिटल हस्ताक्षर प्रमाणपत्रों के संबंध में अनुमानों के लिए व्यवस्था करती हैं। • धारा 34 और 35 इलेक्ट्रानिक रूप में अभिलेखों के अनुरक्षण के लिए व्यवस्था करती हैं।
कंपनी अधिनियम, 2013 और उसके अधीन बनाये गये नियम धारा 2(42) कंपनी लेखा नियम	• इलेक्ट्रानिक रूप में अनुरक्षित लेखा-बहियाँ और अन्य संगत बहियाँ भारत में पहुँच-योग्य रहेंगी। • भारत के बाहर किसी भी स्थान सहित इलेक्ट्रानिक रूप में अनुरक्षित लेखा-बहियों का बैक-अप, बैक-अप आवधिक तौर पर भारत में भौतिक रूप में स्थित सर्वरों पर रखा जाना चाहिए।	• लेखा-बहियों को इलेक्ट्रानिक रूप में अनुरक्षित किये जाने की अनुमति दी गई है, तथापि यदि अभिलेख भारत के बाहर रखे जाते हैं तो बैक-अप सहित भारत में उसकी अभिगम्यता के लिए पर्याप्त प्रक्रिया और प्रणाली उपलब्ध। • यदि लेखा-बहियाँ अपेक्षित कार्यालय स्थान से अलग अन्य स्थानों पर अनुरक्षित की जाती हैं, तो सर्वर का विवरण आरओसी को प्रस्तुत किया जाना चाहिए।
व्यापार-चिह्न (ट्रेडमार्क)	• साइबर स्क्वाटिंग के विरुद्ध संरक्षण • ट्रेडमार्क का उल्लंघन / टीएम अधिनियम की धारा 135 का पारित होना • आईसीएएनएन क्षेत्र (डोमेन) नाम विवाद समाधान	• उल्लंघन और पारित होने (पासिंग आफ़) के लिए कानूनी उपचारात्मक उपाय उपलब्ध हैं। • वेबसाइट आदि का लिंकिंग करते समय चेतावनी दी जानी चाहिए • आईसीएएनएन के अंतर्गत राहत प्राप्त की जा सकती है, यदि (i) प्रतिवादी क्षेत्र (डोमेन) का नाम एकसमान हो (ii) प्रतिवादी के पास कोई

	नीति • मेटा टैगिंग और हाइपर लिंकिंग	विधिसम्मत हित न हो (iii) प्रतिवादी क्षेत्र (डोमेन) का नाम बदनीयती से पंजीकृत किया गया हो • आईपी जोखिम का आकलन किया जाना चाहिए और आईपी उल्लंघन से निपटने के लिए उपयुक्त रणनीति अपनाई जानी चाहिए
प्रतिलिप्यधिकार (कापीराइट) कानून	• डेटाबेस का संरक्षण	• डेटा बेसों का संरक्षण धारा 13 सीए अधिनियम का अक्षरशः पालन करते हुए किया जाता है • साफ्टवेयर प्रोग्रामों का संरक्षण सीए अधिनियम के अधीन किया जा सकता है। अक्षरशः पालन में कंप्यूटर प्रोग्राम धारा 2(1)(ओ) शामिल है। • प्रतिलोम (रिवर्स) इंजीनियरिंग की अनुमति दी गई है - सीए अधिनियम की धारा 51(1)(क)(ग) (उपयोगकर्ता की पहचान के लिए) • आईटी अधिनियम की धारा 43(ख) के अंतर्गत डेटा बेस में अनधिकृत प्रवेश दंडनीय है
गुप्तता और निगरानी	• संविधान के अनुच्छेद 21 अर्थात् गुप्तता के अधिकार के अंतर्गत अंतर्निहित रूप में संरक्षित • यथापरिभाषित आईटी नीति के अनुसार उचित निगरानी की अनुमति दी गई है • डेटा संरक्षण और	राष्ट्रीय साइबर नीति 2013 निम्नलिखित उद्देश्यों के साथ बनाई गई है एक राष्ट्रीय स्तर की नोडल एजेंसी का निर्माण करना जो देश में साइबर सुरक्षा से संबंधित सभी विषयों का समन्वय करेगी • अंतरराष्ट्रीय सर्वोत्तम प्रथाओं के अनुसार संस्थाओं को अपनी स्वयं की सुरक्षा नीतियाँ विकसित करने के लिए प्रोत्साहित करना। उक्त नीति यह सुनिश्चित करेगी कि सभी संस्थाएँ अपनी सुरक्षा नीतियों और पहलों का कार्यान्वयन करने के लिए

	गुप्तता को आईपीसी, 1860, भारतीय संविदा अधिनियम, 1871, विनिर्दिष्ट अनुतोष अधिनियम, 1963 तथा प्रत्यय विषयक जानकारी कंपनी (विनियमन) अधिनियम, 2005 के अंतर्गत भी संरक्षण दिया गया है।	तथा एक बीमा रूपरेखा निर्मित करने के लिए एक विशिष्ट बजट निश्चित करेंगी। • साइबर सुरक्षा संबंधी सर्वोत्तम प्रथाओं, मानकों और दिशानिर्देशों के अनुपालन का प्रमाणीकरण • साइबर क्षेत्र में प्रौद्योगिकीगत गतिविधियों से उत्पन्न होनेवाली साइबर सुरक्षा चुनौतियों का समाधान करने के लिए कानूनी ढाँचा निर्मित किया जाएगा। • 24 x 7 परिचालनगत राष्ट्र स्तरीय कंप्यूटर आपाती प्रतिक्रिया टीम (सर्ट-इन)
भारतीय दंड संहिता 1860 - अपराध	• इलेक्ट्रानिक अभिलेखों की जालसाजी धारा 463 और 468 • झूठा इलेक्ट्रानिक अभिलेख बनाना धारा 464 • गलत इलेक्ट्रानिक अभिलेखों की जालसाजी करना धारा 192 • जाली इलेक्ट्रानिक अभिलेख कब्जे में रखना धारा 474	• आईपीसी के अंतर्गत की गई व्यवस्था के अनुसार **इलेक्ट्रानिक अभिलेखों** की जालसाजी संबंधी समर्थकारी उपबंध • आईटी अधिनियम के संबंधित उपबंध अपराधों की न्यायिक जाँच करने के लिए प्रवर्तन विधि में लागू किये गये हैं।

****