21/02/2024

उत्तराखण्ड शासन
सूचना प्रौद्योगिकी, सुराज एवं विज्ञान प्रौद्योगिकी अनु0–1
संख्या– 214 /XXXIV-1/2024-37/2021 (ई–14316)
देहरादून : दिनांक 21 फरवरी, 2024

अधिसूचना

राज्य डाटा सेंटर, आई0टी0डी0ए0, देहरादून और उसमें स्थापित (hosted) किए गए उपकरण/एप्लिकेशन की सुरक्षा, राज्य के समस्त विभागों को सर्वोत्तम तरीके से सेवा प्रदान करने एवं उपकरणों/एप्लिकेशन्स/डाटा तक अनधिकृत व्यक्तियों की पहुंच को प्रतिबंधित किये जाने के उद्देश्य से 'उत्तराखण्ड राज्य डाटा सेन्टर नीति, 2024' प्रख्यापित किये जाने की श्री राज्यपाल सहर्ष स्वीकृति प्रदान करते है।

संलग्न– यथोपरि।

का0/पु0 (शैलेश बगौली)
सचिव।

संख्या– /XXXIV-1/2024-37/2021 (ई–14316) दिनांक उक्तवत्।

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

1. समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव/सचिव (प्रभारी), उत्तराखण्ड शासन।
2. वरिष्ठ प्रमुख निजी सचिव, मुख्य सचिव, उत्तराखण्ड शासन को मुख्य सचिव महोदय के संज्ञानार्थ।
3. निजी सचिव, मा0 मुख्यमंत्री जी को मा0 मुख्यमंत्री जी के संज्ञानार्थ।
4. निदेशक, मुद्रण एवं लेखन सामग्री राजकीय मुद्रणालय, रूडकी को इस आशय के साथ कि उक्त अधिसूचना को उत्तराखण्ड आगामी असाधारण गजट में प्रकाशित कर उनकी 50–50 प्रतियां सचिव, सूचना एवं विज्ञान प्रौद्योगिकी, उत्तराखण्ड शासन को उपलब्ध कराना सुनिश्चित करें।
5. निदेशक, आई0टी0डी0ए0 देहरादून को इस निर्देश के साथ कि उक्त अधिसूचना को विभाग की वेबसाइट पर जनसामान्य के संज्ञानार्थ अपलोड करते हुये आवश्यक अग्रेत्तर कार्यवाही करने का कष्ट करें।
6. गार्ड फाइल।

आज्ञा से,

का/पु0 (डॉ0 आशीष कुमार श्रीवास्तव)
अपर सचिव।

उत्तराखण्ड शासन
सूचना प्रौद्योगिकी, सुराज एवं विज्ञान प्रौद्योगिकी अनु0–1
संख्या– 214 /XXXIV-1/2024-37/2021 (ई–14316)
देहरादून : दिनांक 21 फरवरी, 2024

अधिसूचना

राज्य डाटा सेंटर, आई0टी0डी0ए0, देहरादून और उसमें स्थापित (hosted) किए गए उपकरण/एप्लिकेशन की सुरक्षा, राज्य के समस्त विभागों को सर्वोत्तम तरीके से सेवा प्रदान करने एवं उपकरणों/एप्लिकेशन्स/डाटा तक अनधिकृत व्यक्तियों की पहुंच को प्रतिबंधित किये जाने के उद्देश्य से 'उत्तराखण्ड राज्य डाटा सेन्टर नीति, 2024' प्रख्यापित किये जाने की श्री राज्यपाल सहर्ष स्वीकृति प्रदान करते है।

संलग्न– यथोपरि।

(शैलेश बगौली)
सचिव।

संख्या– /XXXIV-1/2024-37/2021 (ई–14316) दिनांक उक्तवत्।

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

1. समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव/सचिव (प्रभारी), उत्तराखण्ड शासन।
2. वरिष्ठ प्रमुख निजी सचिव, मुख्य सचिव, उत्तराखण्ड शासन को मुख्य सचिव महोदय के संज्ञानार्थ।
3. निजी सचिव, मा0 मुख्यमंत्री जी को मा0 मुख्यमंत्री जी के संज्ञानार्थ।
4. निदेशक, मुद्रण एवं लेखन सामग्री राजकीय मुद्रणालय, रूडकी को इस आशय के साथ कि उक्त अधिसूचना को उत्तराखण्ड आगामी असाधारण गजट में प्रकाशित कर उनकी 50–50 प्रतियां सचिव, सूचना एवं विज्ञान प्रौद्योगिकी, उत्तराखण्ड शासन को उपलब्ध कराना सुनिश्चित करें।
5. निदेशक, आई0टी0डी0ए0 देहरादून को इस निर्देश के साथ कि उक्त अधिसूचना को विभाग की वेबसाइट पर जनसामान्य के संज्ञानार्थ अपलोड करते हुये आवश्यक अग्रेत्तर कार्यवाही करने का कष्ट करें।
6. गार्ड फाइल।

आज्ञा से,

(डॉ0 आशीष कुमार श्रीवास्तव)
अपर सचिव।

e-ITDA-PRJ/SDC1/8/2020-SEMT-O/o Director ITDA
58036/2024/PROJECTS

उत्तराखण्ड शासन

उत्तराखण्ड राज्य डाटा सेंटर (यूकेएसडीसी) नीति, 2024

सूचना एवं विज्ञान प्रौद्योगिकी विभाग

उत्तराखण्ड शासन

विषय सूची

क्रम संख्या	विषय	पृष्ठ संख्या
1	अध्याय –1: प्रारंभिक	4
2	अध्याय–2: परिचय	5
3	अध्याय–3: प्रयोजन	5
4	अध्याय –4: प्रयोज्यता, स्वामित्व और रूपांतरण	5
5	अध्याय–5: परिकल्पना एवं ध्येय:	6
6	अध्याय–6: उद्देश्य:	6
7	अध्याय –7: भौतिक और पर्यावरण सुरक्षा:	6
8	अध्याय –8: डाटा सेंटर अभिगम:	16
9	अध्याय–9: वर्चुअल प्राइवेट नेटवर्क (वी.पी.एन.)	21
10	अध्याय–10: सर्वर सुरक्षा:	23
11	अध्याय –11: होस्टिंग वातावरण, आवंटन:	26
12	अध्याय–12: पैच प्रबंधन:	28
13	अध्याय–13: परिसंपत्ति प्रबंधन:	32
14	अध्याय–14: बैकअप और पुनर्स्थापना:	38
15	अध्याय –15: लॉग प्रतिधारण:	44
16	अध्याय–16: डाटा हानि रोकथाम (डी.एल.पी.)	47
17	अध्याय–17: लॉगिन सुरक्षा:	50
18	अध्याय–18: एंटीवायरस:	52
19	अध्याय–19: पासवर्ड:	57
20	अध्याय–20: अभिगम नियंत्रण:	62
21	अध्याय–21: एप्लिकेशन सुरक्षा:	68
22	अध्याय–22: परिवर्तन प्रबंधन:	75
23	अध्याय–23: डाटाबेस सुरक्षा:	80
24	अध्याय–24: डेस्कटॉप सुरक्षा:	85
25	अध्याय–25: फायरवॉल:	89

26	अध्याय–26: सूचना सुरक्षा घटना प्रबंधन:	94
27	अध्याय–27: सूचना संचालन, लेबलिंग और निस्तारण:	96
28	अध्याय 28: अनुश्रवण:	103
29	अध्याय 29: नेटवर्क सुरक्षा:	106
30	अध्याय 30: ऑपरेटिंग सिस्टम सुरक्षा:	110
31	अध्याय–31: स्वीकार्य उपयोग:	113
32	अध्याय–32: आपदा पुनर्प्राप्ति (डीआर):	115

अध्याय –1: प्रारंभिक

उत्तराखण्ड स्टेट डाटा सेंटर (यूकेएसडीसी) नीति, 2024 निम्नानुसार है:–

संक्षिप्त नाम, विस्तार एवं प्रारम्भ:

1. (1) इस नीति का संक्षिप्त नाम **"उत्तराखण्ड राज्य डाटा सेंटर (यूकेएसडीसी) नीति, 2024"** है।

(2) यह समस्त राज्य डाटा सेंटर, सूचना प्रौद्योगिकी विकास एजेंसी (आईटीडीए), उत्तराखण्ड पर लागू होगी।

(3) उत्तराखण्ड राज्य डाटा सेंटर (यूकेएसडीसी) नीति–2024", इसके प्रकाशन की तिथि से प्रवृत्त होगी।

2. परिभाषाएँ:

उत्तराखण्ड राज्य डाटा सेंटर (यूकेएसडीसी) नीति, 2024 में निम्नलिखित परिभाषाएँ लागू होंगी:

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 अभिप्रेत है;

(ख) "बीआईए" से व्यवसाय प्रभाव विश्लेषण अभिप्रेत है;

(ग) "सीसीटीवी." से क्लोज्ड–सर्किट टेलीविजन अभिप्रेत है;

(घ) "सीआईएसओ" से मुख्य सूचना सुरक्षा अधिकारी अभिप्रेत है;

(ङ) "डीसीओ" से डाटा सेंटर ऑपरेटर अभिप्रेत है;

(च) "डीएलपी" से डाटा हानि की रोकथाम अभिप्रेत है;

(छ) "डीएमजेड" से विसैन्यीकृत क्षेत्र अभिप्रेत है;

(ज) "जी.ओ.यूके" से उत्तराखंड सरकार अभिप्रेत है;

(झ) "आईपीसेक" का तात्पर्य इंटरनेट प्रोटोकॉल सुरक्षा अभिप्रेत है;

(ञ) "आईआरटी." से घटना प्रतिक्रिया टीम अभिप्रेत है;

(ट) "आईटीडीए" से सूचना प्रौद्योगिकी विकास एजेंसी अभिप्रेत है;

(ठ) "एल2टीपी" से लेयर 2 टनलिंग प्रोटोकॉल अभिप्रेत है;

(ड) "एमईआईटीवाई" से इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय अभिप्रेत है;

(ढ) "संगठन/विभाग" से उत्तराखंड सरकार के संगठन और विभाग, निगम, संस्थान, प्राधिकरण, सोसायटी, निदेशालय, बोर्ड और सरकार के ऐसे अन्य संगठन अभिप्रेत हैं;

(ण) "राज्य सरकार" से उत्तराखंड राज्य सरकार अभिप्रेत है;

(त) "आरए" से जोखिम मूल्यांकन अभिप्रेत है;

(थ) "एसडीसी" से राज्य डाटा सेंटर अभिप्रेत है;

(द) "एसएनएमपी" से सरल नेटवर्क प्रबंधन प्रोटोकॉल अभिप्रेत है;

(ध) "एसओपी." का तात्पर्य "मानक संचालन प्रक्रिया" अभिप्रेत है;

(न) "यूकेएसडीसी" का तात्पर्य उत्तराखंड राज्य डाटा सेंटर अभिप्रेत है;

(प) "वीपीएन" से वर्चुअल प्राइवेट नेटवर्क अभिप्रेत है;

अध्याय–2: परिचय

3.1 उत्तराखण्ड राज्य डाटा सेंटर (यूकेएसडीसी) नागरिकों को अधिक विश्वसनीयता, उपलब्धता और सेवा क्षमता के साथ सेवाएं प्रदान करने के लिए ई–शासन की पहल एवं व्यवसायों/सरोकारों का एक प्रमुख सहायक तत्व है। यूकेएसडीसी बेहतर संचालन और प्रबंधन नियंत्रण प्रदान करता है तथा डाटा प्रबंधन, आईटी प्रबंधन, परियोजना और अन्य मूल्यों की समग्र लागत को कम करता है।

3.2 सूचना प्रौद्योगिकी विकास एजेंसी (आईटीडीए), सूचना एवं विज्ञान प्रौद्योगिकी विभाग, उत्तराखण्ड सरकार द्वारा प्रबंधित उत्तराखण्ड राज्य डाटा सेंटर (यूकेएसडीसी) का प्राथमिक कार्य उत्तराखण्ड शासन के विभिन्न विभागों को आईटी सेवाओं के प्रावधान के लिए आवश्यक विभिन्न प्रकार के अनुप्रयोगों, डाटा तथा उपकरणों के स्थापन हेतु एक सुरक्षित, लचीला, अभियांत्रिक एवं निगरानी वाला वातावरण प्रदान करना है, जो उत्तराखण्ड सरकार के कई व्यवसाय की सफल पूर्ति के लिए महत्वपूर्ण हैं।

अध्याय–3: प्रयोजन

4. उत्तराखण्ड राज्य डाटा सेंटर (यूकेएसडीसी) नीति का प्रयोजन यह सुनिश्चित करने में सहायता करना है कि डाटा सेंटर, और उसमें स्थापित (hosted) किए गए उपकरण/एप्लिकेशन सुरक्षित, सही आकार में और सभी सरकारी विभागों को सर्वोत्तम तरीके से सेवा देने व अनधिकृत व्यक्तियों के डाटा सेंटर तक पहुंच प्रतिबंधित करने की प्रक्रियाओं हेतु ईष्टतम् रूप से प्रावधानित हैं।

अध्याय –4: प्रयोज्यता, स्वामित्व एवं रूपांतरण

5.1 यूकेएसडीसी की यह नीति उत्तराखंड राज्य डाटा सेंटर, सूचना प्रौद्योगिकी विकास एजेंसी (आईटीडीए), सूचना और विज्ञान प्रौद्योगिकी विभाग, उत्तराखंड सरकार पर लागू होगी।

5.2 यूकेएसडीसी नीति का स्वामित्व सूचना प्रौद्योगिकी विकास एजेंसी (आईटीडीए), सूचना और विज्ञान प्रौद्योगिकी विभाग, उत्तराखंड सरकार के पास है।

5.3 आवश्यकता पड़ने पर नीति को नियमित आधार पर अद्यतन किया जायेगा।

5.4 आईटीडीए इस यूकेएसडीसी नीति के कार्यान्वयन के लिए किसी भी योजना, संशोधन, जोडना, रूपांतरण, विलोपन, पुनरीक्षण आदि करने का हकदार होगा जो सूचना प्रौद्योगिकी विकास एजेंसी (आईटीडीए), सूचना और विज्ञान प्रौद्योगिकी विभाग, उत्तराखंड सरकार द्वारा जारी किया जाएगा।

5.5 यह नीति डाटा सेंटर स्थापित करने वाले राज्य के किसी भी विभाग के लिए मार्गदर्शक नीति के रूप में कार्य करेगी।

अध्याय–5: परिकल्पना एवं ध्येय

6. परिकल्पना: उत्तराखंड राज्य के सुरक्षित, सुदृढ़ और लचीला होस्टिंग वातावरण को सुविधाजनक बनाने और बढ़ती मांग को पूरा करने और नागरिकों को अत्याधुनिक सेवा वितरण की सुविधा के लिए डाटा के विश्वसनीय होस्टिंग अवसंरचना के प्रावधान को सक्षम करना है।

7. ध्येय:

1. उत्तराखंड राज्य में स्थायी और विश्वसनीय डाटा सेंटर क्षमता सुनिश्चित करना।
2. अत्याधुनिक डाटा सेंटरों की स्थापना को सुगम बनाना।

अध्याय–6: उद्देश्य

इस यूकेएसडीसी नीति के माध्यम से संचालित किए जाने वाले कुछ प्रमुख उद्देश्य निम्नलिखित हैं:

8.1 उत्तराखंड में डाटा के लिए सुरक्षित और सुदृढ़ डाटा होस्टिंग वातावरण के लिए आवश्यक नियामक, संरचनात्मक और प्रक्रियात्मक हस्तक्षेप परिचालित करना।

8.2 सरकार की नीति के अनुसार डाटा सेंटर के विकास में मानकीकरण की सुविधा प्रदान करना।

8.3 एस.डी.सी. में होस्ट किए गए डाटा की सुरक्षा सुनिश्चित करना।

8.4 राज्य सरकार के विभाग, निगमों और सार्वजनिक क्षेत्र की ईकाइयों की होस्टींग की सुविधा के लिए तंत्र का विकास करना।

अध्याय –7: भौतिक एवं पर्यावरण सुरक्षा

9. (क) प्रयोजन:

इस नीति का प्रयोजन उत्तराखंड राज्य डाटा सेंटर (यूकेएसडीसी) को सुरक्षित करने के लिए भौतिक और पर्यावरण सुरक्षा स्थापित करना है। भौतिक और पर्यावरण सुरक्षा नीति, यूकेएसडीसी की सूचना प्रणाली और भौतिक और पर्यावरणीय खतरों से प्रसंस्करण सुविधाओं की सुरक्षा को बनाए रखने के लिए आवश्यक उपयुक्त सुरक्षा नियंत्रणों के विकास और कार्यान्वयन के लिए दिशा प्रदान करती है। इस नीति का उद्देश्य होस्ट किए गए विभाग की सूचना प्रणालियों की सुरक्षा के लिए जोखिम को कम करना और डाटा सेंटर के भीतर कार्य करने वाले कर्मचारियों की सुरक्षा सुनिश्चित करने में मदद करना है।

(ख) नीति कथन/विवरण और उद्देश्य:

यूकेएसडीसी और सुविधाओं को अनधिकृत भौतिक पहुंच और पर्यावरणीय खतरों के विरुद्ध पर्याप्त सुरक्षा प्रदान की जाएगी। यूकेएसडीसी की सूचना प्रणालियों और उपकरणों की सुरक्षा और पर्याप्तता बनाए रखने के लिए उपयुक्त सुरक्षा नियंत्रण लागू किए जाएंगे। नीति का उद्देश्य यूकेएसडीसी सूचना प्रणाली को अनधिकृत भौतिक पहुंच और पर्यावरणीय खतरों से सुरक्षित करना है।

(ग) नियंत्रण:

1. यूकेएसडीसी नीति सुनिश्चित करती है कि सुरक्षित क्षेत्रों के लिए प्रक्रियाएं उचित प्रवेश नियंत्रणों द्वारा संरक्षित हैं ताकि यह सुनिश्चित किया जा सके कि केवल अधिकृत कर्मियों को ही पहुंच की अनुमति है और भौतिक साइट केवल अधिकृत कर्मचारियों या विभाग के प्रमुख या इसके प्राधिकृत अधिकारी द्वारा अधिकृत नामित उपयोगकर्ताओं तक पहुंच के लिए सीमित होगी। एक्सेस कंट्रोल के लिए आवश्यक एक्सेस मैकेनिज्म का उपयोग किया जाएगा और निम्नलिखित मानक को विकसित और बनाए रखना चाहिए:
   (एक) पहुँच का अनुरोध और अनुमोदन करने के लिए प्रक्रियाओं की स्थापना करना।
   (दो) डाटा सेंटर संपत्ति वस्तुसूची बनाए रखना।
   (तीन) डाटा सेंटर सुरक्षा दिशानिर्देश बनाना और पोस्ट करना।
   (चार) अधिकृत व्यक्तियों की सूची बनाए रखना।
2. यूकेएसडीसी डाटा सेंटर और उसके उपकरणों के उचित संचालन को सुनिश्चित करने और नुकसान को कम करने के लिए, सभी डाटा सेंटर एसेट को डाटा सेंटर एसेट इन्वेंटरी पर ट्रैक और मॉनिटर किया जाना चाहिए।
3. सीसीटीवी कैमरों की तरह निगरानी प्रणाली का उपयोग करके भौतिक साइट और डाटा सेंटर की निगरानी की जाएगी और उसमें गतिविधियों को रिकॉर्ड किया जाएगा। यूकेएसडीसी सारणी के अनुसार, वीडियो कम से कम (30) दिनों तक बनाए रखा जाएगा।
4. डाटा सेंटर में यूपीएस, डीजल जेनरेटर इत्यादि जैसी उचित बिजली आपूर्ति नियंत्रण प्रणाली होनी चाहिए। सहायक उपयोगिता विफलता की स्थिति में बैकअप (यूपीएस और डीजल जेनरेटर) के लिए उचित प्रावधान करके उपकरण को बिजली की विफलता से संरक्षित किया जाना चाहिए।
5. एएमसी ठेकेदार द्वारा कम से कम त्रैमासिक रूप से अग्नि संसूचक प्रणाली, गैस दमन, सीसीटीवी, एक्सेस कंट्रोल सिस्टम आदि का परीक्षण किया जाएगा।
6. केबलिंग सुरक्षा: संवेदनशील डाटा और सहायक सेवाओं को ले जाने वाली पावर और फाइबर केबलिंग को अवरोधन या क्षति से बचाया जाना चाहिए। केबल प्रवेश मार्ग को अच्छी तरह परिभाषित और संरक्षित किया जाना चाहिए।
7. गैर–सार्वजनिक डाटा वाले आवास प्रणालियों को लॉक रखने के लिए एस.डी.सी. की उचित भौतिक सुरक्षा को लागू किया जाएगा।
8. प्राकृतिक, या मानव निर्मित आपदाओं, जैसे आग, बाढ़, विस्फोट आदि से होने वाली क्षति के विरूद्ध उचित सुरक्षा लागू की जाएगी।
9. यह सुनिश्चित करने के लिए प्रक्रियाएं मौजूद हैं कि उपकरण स्थानांतरित या स्क्रैप किए जाने पर किसी भी संवेदनशील डाटा और लाइसेंस प्राप्त सॉफ्टवेयर को हटा दिया गया है या सुरक्षित रूप से अधिलेखित कर

दिया गया है और किसी भी उपकरण को डाटा सेंटर के अंदर या बाहर ले जाने से पहले उसे विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा अनुमोदित किया जाना चाहिए, साथ ही डिवाइस (यंत्र) विवरण अभिलिखित किया जाना चाहिए।

10. डाटा सेंटर सुरक्षा नीति, जहां तक संभव हो, भौतिक वातावरण को सुरक्षित करने में अच्छे अभ्यास का पालन करना चाहती है, जिसमें नेटवर्किंग, सर्वर, स्टोरेज और अन्य हार्डवेयर होते हैं जो उत्तराखंड सरकार के होस्टेड डिपार्टमेंट एप्लिकेशन / डाटा सूचना और संचार सेवाओं को आधार प्रदान करते हैं।
11. सैद्धान्तिक रूप में, डाटा सेंटर के वातावरण का उद्देश्य डाटा सेंटर के भीतर होस्ट किए गए सर्वर जितना सुरक्षित होना है। सुरक्षा प्रणाली की विश्वसनीयता की जांच के लिए अर्धवार्षिक/वार्षिक समीक्षा और मॉक ड्रिल आयोजित की जाएगी।

10. भौतिक सुरक्षा मापदण्ड

यह खंड संवेदनशील आईटी सुविधाओं को अनधिकृत पहुंच से बचाने के लिए भौतिक नियंत्रणों के संकेंद्रित परतों की आवश्यकता का वर्णन करता है।

11. सार्वजनिक पहुंच, वितरण और लोडिंग क्षेत्रः

(एक) यह सुनिश्चित किया जाएगा कि सभी क्षेत्रों, जहां वस्तुओं की लोडिंग और अनलोडिंग की जाती है, की निगरानी की जाती है, और इन गतिविधियों के दौरान उचित भौतिक सुरक्षा नियंत्रणों से सुसज्जित किया जाता है।

(दो) इन क्षेत्रों में प्रवेश केवल चिन्हित और अधिकृत कर्मियों तक ही सीमित होगा।

12. विद्युत आपूर्ति

सभी उपकरणों को विद्युत विफलताओं और सहायक उपयोगिताओं में विफलताओं के कारण होने वाले अन्य व्यवधानों से संरक्षित किया जाना चाहिए। यह सुनिश्चित किया जाएगा कि:

(एक) विद्युत, जलापूर्ति, सीवेज, हीटिंग/वेंटिलेशन, तथा एयर कंडीशनिंग (वातानुकूलन) जैसी सभी सहायक उपयोगिताओं, सूचना प्रणालियों और/या प्रसंस्करण सुविधाओं हेतु उपयुक्त स्थिति में हैं जिनका वे समर्थन कर रहे हैं।

(दो) यूकेएसडीसी कार्य संचालन के सहायक उपकरणों के निरंतर क्रिया का समर्थन करने हेतु निर्बाध विद्युत आपूर्ति (यू.पी.एस.) सिस्टम और जनरेटर स्थापित किए गए हैं।

(तीन) यू.पी.एस. को उपकरण निर्माता की संस्तुति के अनुसार अनुरक्षित किया जाएगा।

(चार) यूकेएसडीसी के सभी परिसरों में इलेक्ट्रिक सर्ज को रोकने के लिए उचित अर्थिंग होनी चाहिए।

(पाँच) सहायक उपयोगिताओं में खराबी को उजागर करने के लिए एक अलार्म सिस्टम स्थापित किया गया है।

(छः) विद्युत उतार–चढ़ाव से बचाव के लिए, जहां कहीं आवश्यक हो, वोल्टेज नियामक स्थापित किए जाएंगे। हार्डवेयर को विद्युत उतार–चढ़ाव या शॉर्ट सर्किट से बचाने के लिए उपयुक्त क्षमता के सर्किट ब्रेकर लगाए जाने चाहिए।

(सात) उपयोगिता उपकरणों के लिए नियमित अंतराल पर एक पूर्व–सतर्कता–संबंधी रखरखाव अभ्यास किया जाता है।

13. यूकेएसडीसी के लिए भौतिक सुरक्षा

(I) सुरक्षा क्षेत्र

जनता, आगंतुकों, हितधारकों, ठेकेदारों और यूकेएसडीसी के कर्मचारियों के अनुसार क्षेत्रों को विभाजित और स्पष्ट रूप से श्रेणियों में परिभाषित किया जाना चाहिए। ताकि, संपत्तियों और संवेदनशील सूचनाओं की सुरक्षा के लिए एक प्रभावी सुरक्षा तंत्र बनाया जा सके। परिसर को निम्नलिखित क्षेत्रों में वर्गीकृत किया जाना चाहिए:

1. सार्वजनिक क्षेत्र: एक सार्वजनिक क्षेत्र आम तौर पर आईटीडीए भवन का एक हिस्सा होता है जहां जनता, हितधारक तथा आगंतुक किसी भी समय आ सकते हैं। उदाहरणों में मुख्य द्वार, स्वागत कक्ष, लॉबी एवं आगंतुक कक्ष शामिल हैं।
   (क) सभी हितधारकों को कर्मचारियों, आगंतुक, हितधारकों, विक्रेताओं, ठेकेदारों तथा परामर्शदाताओं में वर्गीकृत किया जाना चाहिए। मुख्य द्वार पर सुरक्षा गार्डों को आगंतुक से उनकी भेंट के उद्देश्य के बारे में पूछना चाहिए। संबंधित यूकेएसडीसी कर्मचारी द्वारा पुष्टि के बाद, आगंतुक को विज़िटर फॉर्म या विज़िटर रजिस्टर भरना चाहिए, सुरक्षा गार्ड द्वारा विज़िटर आईडी कार्ड जारी किया जाएगा, और गार्ड द्वारा आगंतुक को परिसर में प्रवेश की अनुमति दी जाएगी।
   (ख) मुख्य द्वार/द्वार से आने–जाने वाले आगंतुकों की निगरानी सीसीटीवी से की जानी चाहिए।
   (ग) नियमित आपूर्तिकर्ताओं/विक्रेताओं/हितधारकों को स्वतंत्र रजिस्टरों में सूचीबद्ध किया जाना चाहिए और सुरक्षा कर्मियों को सुविधा में अनुमति देने से पहले उनके नाम और पहचान की पुष्टि करनी चाहिए।
   (घ) आगंतुकों को आगंतुकों की लॉग बुक/रजिस्टर में साइन–इन करना चाहिए। यदि संभव हो तो सुरक्षा गार्ड/प्रशासन विभाग द्वारा दैनिक/साप्ताहिक समीक्षा की जानी चाहिए।
   (ङ) सुरक्षा गार्ड को सभी आवक और जावक सामग्री तथा अनुरक्षण हेतु भेजे जाने वाले अन्य उपकरणों की प्रविष्टि आवक/जावक रजिस्टर में करनी चाहिए।
   (च) यूकेएसडीसी भवन से आने वाले और बाहर जाने वाले उपकरणों के लिए गेट पास जारी किया जाना चाहिए। गेट पास के बिना प्रवेश प्रतिबंधित होना चाहिए।
   (छ) प्रशासन विभाग या सुरक्षा गार्ड को यह सुनिश्चित करना चाहिए कि सभी हितधारक आईटीडीए सुविधाओं में रहते हुए आईटीडीए आई.डी. कार्ड / विज़िटर आई.डी. इस प्रकार से पहनें कि यह हर समय स्पष्ट रूप से प्रदर्शित हो ताकि भौतिक सुरक्षा कर्मियों को यूकेएसडीसी के कर्मचारियों की पहचान सत्यापित करने में सुविधा हो। आई.डी.– कार्ड सभी को दिखना चाहिए।
   (ज) सुरक्षा गार्डों को सुरक्षा जागरूकता प्रशिक्षण दिया जाना चाहिए।
   (झ) सभी हितधारकों को आईटीडीए के प्रशासनिक विभाग से पूर्व लिखित अनुमति लेनी होगी।
   (ञ) सभी हितधारक जो अपना पहचान–पत्र भूल जाते हैं, उन्हें स्वागत डेस्क पर साइन इन करना होगा और उन्हें एक अस्थायी पहचान–पत्र प्राप्त होगा।
   (ट) सभी हितधारकों को अपनी कंपनी का आई.डी.–कार्ड अपने साथ रखना चाहिए जब वे आईटीडीए की सुविधा ले रहे हों।

(II) **प्रतिबंधित क्षेत्रः** एक प्रतिबंधित क्षेत्र एक ऐसा क्षेत्र है जहां पहुंच अधिकृत व्यक्तियों तक सीमित है और व्यावसायिक आवश्यकता के मामले में, सभी हितधारकों को उनके कार्य क्षेत्र में उचित रूप से अनुरक्षित किया जाना चाहिए। उदाहरण में डाटा सेंटर शामिल हैं।

(क) सभी आगंतुकों को प्रतिबंधित क्षेत्रों में अधिकृत कर्मियों द्वारा एस्कॉर्ट किया जाना चाहिए।

(ख) डाटा सेंटर में प्रवेश करने के लिए अधिकृत कर्मचारियों की एक सूची (जैसा कि आईटीडीए द्वारा अनुमोदित है) यूकेएसडीसी टीम द्वारा तैयार और बनाए रखा जाना चाहिए।

(ग) यदि किसी आगंतुक को प्रतिबंधित क्षेत्र के अंदर लैपटॉप, पामटॉप, कैमरा और कोई अन्य डाटा–कैप्चरिंग (ऑडियो/वीडियो) उपकरण ले जाने की आवश्यकता होती है, तो सुरक्षा गार्ड को इन उपकरणों के सीरियल नंबर, मेक, मॉडल आदि जैसे आवश्यक विवरण भी नोट करने चाहिए।

(घ) किसी भी समस्या के मामले में आईटीडीए उन उपकरणों की जांच कर सकता है, जिन्हें आवश्यकता पड़ने पर डाटा सेंटर के अंदर ले जाया गया था।

(ङ) चौबीसों घंटे महत्वपूर्ण सुविधाओं की निगरानी के लिए क्लोज सर्किट टीवी (सी.सी.टी.वी.) सहित सतत् निगरानी प्रणाली स्थापित की जानी चाहिए।

(च) प्रतिबंधित क्षेत्रों तक पहुंच अधिकृत कर्मियों के लिए होनी चाहिए और आवश्यकता–से–पहुंच के सिद्धांत को लागू किया जाना चाहिए।

(छ) डाटा सेंटर, एन.ओ.सी., एस.ओ.सी., बी.एम.एस. क्षेत्र आदि तक पहुंच को प्रतिबंधित क्षेत्रों के रूप में वर्गीकृत किया जाना चाहिए।

(ज) प्रतिबंधित क्षेत्र से बाहर निकलते समय संवेदनशील सूचना और संपत्ति को सुरक्षित किया जाना चाहिए। संवेदनशील सूचना के बारे में चर्चा करते समय सावधानी बरतनी चाहिए।

(झ) लाकर और कंटेनरों का उपयोग अप्राप्य संवेदनशील सूचना और संपत्तियों की सुरक्षा के लिए किया जाना चाहिए।

(III) पर्यावरण संरक्षण

1. अग्नि संसूचक तथा नियंत्रण हेतु निम्नलिखित सहित पर्याप्त प्रावधान होने चाहिएः–

(क) सभी महत्वपूर्ण स्थानों पर स्मोक डिटेक्टर और फायर अलार्म लगाए जाने चाहिए।

(ख) आसानी से दिखाई देने वाले और सुलभ स्थानों पर अग्निशामक यंत्र स्थापित किए जाने चाहिए।

(ग) सभी कर्मियों को अग्निशामक यंत्रों के प्रयोग का प्रशिक्षण दिया जाना चाहिए। हर छह माह में मॉक ड्रिल कराई जाए।

(घ) आपातकालीन टेलीफोन नंबर नोटिस बोर्ड और अन्य दृश्य क्षेत्र पर प्रदर्शित किए जाने चाहिए।

(ङ) आपातकालीन निकास को दृश्यमान और ठीक से लेबल किया जाना चाहिए और अवरुद्ध नहीं किया जाना चाहिए।

(च) ज्वलनशील सामग्री को महत्वपूर्ण स्थानों में जैसे डाटा सेंटर, और यू.पी.एस. कक्ष आदि के पास नहीं रखा जाना चाहिए।

(छ) एएमसी ठेकेदार द्वारा कम से कम त्रैमासिक रूप से अग्नि संसूचक, गैस दमन, सी.सी.टी.वी., एक्सेस कंट्रोल सिस्टम आदि का परीक्षण किया जाना चाहिए।

(ज) यह सुनिश्चित करने के लिए प्रक्रियाएं होनी चाहिए कि उपकरण, सूचना या सॉफ्टवेयर को बिना पूर्व अनुमति के ऑफ–साइट न ले जाया जाए।

2. डाटा सेंटर और अन्य प्रतिबंधित क्षेत्र में भी खाने–पीने की चीजों का सेवन पूरी तरह प्रतिबंधित होना चाहिए।

3. उपकरण निर्माता के विनिर्देशों के अनुसार एयर कंडीशनिंग सिस्टम को लागू किया जाना चाहिए।

(क) तापमान और आर्द्रता की निगरानी और नियंत्रण किया जाना चाहिए, यह सुनिश्चित करते हुए कि डाटा सेंटर में तापमान हमेशा 20 से 24 डिग्री सेल्सियस के बीच बनाए रखा जाना चाहिए।

(ख) धूल और संदूषकों को हटाने के लिए हवा को परिचालित और फिल्टर किया जाना चाहिए।

(ग) जहां कहीं भी आवश्यक हो वहां नमी का पता लगाने वाले सिस्टम/डीह्यूमिडि फायर मौजूद होने चाहिए।

4. फर्श, दीवारों, भंडारण अलमारियों और आईटी उपकरणों की समय–समय पर वैक्यूम क्लीनर से सफाई करना आवश्यक है।

5. डाटा सेंटर में पानी और अन्य तरल अग्निशामकों का उपयोग नहीं किया जाना चाहिए, क्योंकि मशीन, टेप और केबल क्षतिग्रस्त हो सकते हैं।

6. भंडारण कक्षों, अभिलेख संग्रह कक्ष आदि में अग्निशामक तंत्र के रूप में पानी और अन्य तरल शामकों का उपयोग नहीं किया जाना चाहिए।

7. यदि संभव हो, तो पानी के रिसाव को रोकने के लिए डाटा सेंटर की छत और दीवारों को रसायनों से पर्याप्त रूप से लेपित किया जाना चाहिए।

8. पहचाने गए खतरों का मुकाबला करने के लिए दरवाजे, खिड़कियां, एक्सेस हैच और सर्विस डक्ट्स को डिजाइन करने की आवश्यकता है। सर्वर या डाटा सेंटर के तल के ऊपर एक कृत्रिम तल का निर्माण किया जाना चाहिए। यह पानी के रिसाव से सुरक्षा प्रदान करेगा। इसके अलावा, यह एम.यू.एक्स. और यू.पी.एस. कक्ष से कर्मियों के आने–जाने में बिना किसी बाधा के नेटवर्क केबल, विद्युत लाइन और टेलीफोन कनेक्शन बिछाने में सक्षम होगा।

9. सभी विद्युत बिंदुओं की पहचान करने के लिए विद्युत अभिन्यास का एक समग्र आरेख तैयार किया जाना चाहिए।

10. फ्लोर लेआउट और सुरक्षित असेंबली पॉइंट का एक समग्र आरेख तैयार किया जाना चाहिए।

11. यूकेएसडीसी के संचालन के लिए महत्वपूर्ण डाटा को संसाधित करने वाली सभी महत्वपूर्ण सुविधाओं के लिए निर्बाध विद्युत प्रणालियां स्थापित की जानी चाहिए। यह सुनिश्चित किया जाना चाहिए कि यू.पी.एस. हमेशा काम करने की स्थिति में हो।

12. विद्युत उतार–चढ़ाव से बचाव के लिए वोल्टेज नियामकों को स्थापित किया जाना चाहिए।

13. पावर वोल्टेज में वृद्धि के विरूद्ध हार्डवेयर की सुरक्षा के लिए उपयुक्त क्षमता के सर्किट ब्रेकर स्थापित किए जाने चाहिए।

14. सामान्य विद्युत लाइनों के विफल होने की स्थिति में विद्युत उत्पादन के लिए जनरेटर उपलब्ध कराए जाने चाहिए।

15. अचानक विद्युत विफलता को संभालने के लिए, डाटा सेंटर और आवश्यकतानुसार किसी अन्य स्थान पर सेल्फ–एक्टिवेटिंग इमरजेंसी लैंप को रखा जाना चाहिए।

16. आकस्मिक सक्रियण से बचने के लिए पर्याप्त लेबलिंग और परिरक्षण के साथ सामरिक स्थानों में आपातकालीन पावर ऑफ स्विच की स्थापना सुनिश्चित करें।

17. निर्दिष्ट व्यक्तियों को उपरोक्त सुरक्षा प्रणालियों का तिमाही में कम से कम एक बार परीक्षण करना चाहिए।

18. सुनिश्चित करें कि स्पष्ट डेस्क नीति लागू है।
19. कागजी संपत्तियों को एक बंद कमरे/कैबिनेट में रखें जहां केवल अधिकृत कर्मियों की ही पहुंच हो।
20. बैकअप टेपों को ऑफसाइट स्थान पर ले जाते समय उनकी सुरक्षा सुनिश्चित करें।

14. अभिगम नियंत्रण

1. डाटा सेंटर, एन.ओ.सी., एस.ओ.सी., बी.एम.एस. सहित महत्वपूर्ण सूचना प्रसंस्करण सुविधाओं में अनधिकृत भौतिक पहुंच के विरूद्ध पर्याप्त सुरक्षा होनी चाहिए। सुरक्षा के लिए निम्नलिखित तंत्रों का उपयोग किया जा सकता है: सुरक्षा गार्ड, ऑटोमेटेड एक्सेस कंट्रोल मैकेनिज्म जैसे बायोमेट्रिक कंट्रोल या एक्सेस कार्ड।
2. सभी कर्मचारियों और आगंतुकों को पहचान पत्र प्रदान किया जाना चाहिए।
   (क) सभी कर्मचारियों के पास फोटो–पहचान पत्र होना चाहिए। यूकेएसडीसी परिसर में प्रवेश करने से पहले तीसरे पक्ष के कर्मियों को पहचान पत्र प्रदान किए जाने चाहिए। एक व्यक्ति को रोका जा सकता है यदि उसने दृश्यमान पहचान पत्र धारण नहीं किया है।
   (ख) एक्सेस कार्ड के गुम होने की सूचना तुरंत प्रशासनिक विभाग को दी जानी चाहिए।
3. महत्वपूर्ण सूचना प्रसंस्करण सुविधाओं तक पहुंच आवश्यक अनुमोदन के बाद ही प्रदान की जानी चाहिए। उदाहरण के लिए, किसी भी व्यक्ति को डाटा सेंटर तक पहुंच की आवश्यकता है, उसे सी.आई.एस.ओ. द्वारा अधिकृत व्यक्ति से पूर्व अनुमोदन प्राप्त करना चाहिए।
4. डाटा सेंटर के सभी रैक बंद कर दिए जाने चाहिए। इन रैकों तक पहुंच केवल अधिकृत कर्मियों तक ही सीमित होनी चाहिए।
5. कागजी संपत्तियों को एक बंद कमरे/कैबिनेट में रखें जहां केवल अधिकृत कर्मियों की ही पहुंच हो।
6. सभी डेस्कटॉप और अन्य उपकरणों को भौतिक टैग और लॉक किया जाना चाहिए।
7. सभी बैकअप टेपों को अग्निरोधक में सुरक्षित रखें।
8. पिग्गी बैकिंग की अनुमति नहीं हो।

15. अनुश्रवण

1. चौबीसों घंटे प्रतिदिन के सापेक्ष महत्वपूर्ण सुविधाओं की निगरानी के लिए क्लोज सर्किट टीवी (सी.सी.टी.वी.) सहित सतत निगरानी प्रणाली स्थापित की जानी चाहिए। पूरे सीसीटीवी सिस्टम के वीडियो को हार्ड डिस्क ड्राइव पर संग्रहित किया जाना चाहिए।
2. सीसीटीवी का बैकअप कम से कम तीस (30) दिनों के लिए रखा जाएगा।
3. किसी भी संदिग्ध गतिविधि के लिए समय–समय पर सीसीटीवी वीडियो की समीक्षा की जानी चाहिए।
4. निगरानी की सुविधा के लिए सभी पहुंच बिंदुओं पर पर्याप्त रोशनी की व्यवस्था की जानी चाहिए।
5. सभी निगरानी उपकरणों को डस्ट–प्रूफ हाउसिंग में रखा जाना चाहिए।
6. बायोमेट्रिक एक्सेस कंट्रोल डिवाइसेज और अन्य एक्सेस कंट्रोल डिवाइसेज के लॉग की समय–समय पर समीक्षा की जानी चाहिए। लॉग को अनधिकृत पहुंच और संशोधन से संरक्षित किया जाना चाहिए।

16. केबलिंग सुरक्षा

1. सूचना प्रसंस्करण सुविधाओं के लिए दूरसंचार लाइन और नेटवर्क केबल भूमिगत होने चाहिए। इसे अनधिकृत अवरोधन और क्षति से संरक्षित किया जाना चाहिए।
   (क) भवन के प्लेनम स्पेस में केबल चलाई जानी चाहिए। सभी केबल बिछाने का काम प्लेनम केबल्स का उपयोग करके किया जाना चाहिए।
   (ख) हस्तक्षेप को रोकने के लिए विद्युत केबलों को संचार केबलों से अलग किया जाना चाहिए।
2. यह दृढ़ता से अनुशंसा की जाती है कि केबल रूटिंग और टर्मिनेशन दिखाने वाले विस्तृत भौतिक नेटवर्क आरेखों सहित अभिलेख यूकेएसडीसी के पास बनाए रखे जाएं।

17. अभिलेख सुरक्षा

1. हार्ड कॉपी और सॉफ्ट कॉपी (सी.डी., फ्लॉपी, टेप आदि) सहित संवेदनशील अभिलेखों को हमेशा बंद कैबिनेट में रखा जाना चाहिए।
2. सभी अभिलेखों के लिए अभिलेख संस्करण नियंत्रण और लेबलिंग का पालन किया जाना चाहिए।
3. सभी आईटी उपकरणों और अन्य उपकरणों की भौतिक सूची और लेबलिंग को बनाए रखा जाना चाहिए।
4. सर्विस लेवल एग्रीमेंट (एस.एल.ए.) और नॉन–डिस्क्लोजर एग्रीमेंट (एन.डी.ए.) को तीसरे पक्ष के विक्रेताओं, ठेकेदारों के साथ हस्ताक्षरित किया जाना चाहिए।
5. यूकेएसडीसी सुविधाओं में सुरक्षा पोस्टर लगाए जाने चाहिए।
6. फैक्स मशीन और प्रिंटर उन क्षेत्रों में स्थापित किए जाने चाहिए जहां अनधिकृत पहुंच का जोखिम कम हो।
   (क) उपयोगकर्ताओं को यह सुनिश्चित करना चाहिए कि जब भी संवेदनशील अभिलेख मुद्रित होते हैं, तो प्रिंटआउट तुरंत एकत्र किए जाते हैं।
   (ख) गोपनीय फैक्स तुरंत एकत्र किया जाना चाहिए।
   (ग) कार्यालय उपकरण और सामग्री का उपयोग व्यक्तिगत कारणों से नहीं किया जाना चाहिए जैसे फोटो प्रिंट करना या फोटो स्कैन करना।

18. डाटा का निस्तारण

1. अभिलेख के स्वामी को यह सुनिश्चित करने की आवश्यकता है, कि आवश्यक उपाय किए गए हैं कि अभिलेख में सूचना के निस्तारण किये जाने के बाद पुनर्प्राप्त नहीं किया जा सकता है। डाटा भंडारण उपकरणों में व्यावसायिक महत्वपूर्ण सूचना होती है। उन पर संग्रहीत डाटा को निस्तारित करने से पूर्व मिटाने की आवश्यकता होती है।
2. अनुरक्षण हेतु भेजने से पहले सर्वर, डेस्कटॉप और लैपटॉप की हार्ड डिस्क को प्रारूपित (फार्मेट) कर दिया जाना चाहिए।
3. डाटा भंडारण उपकरणों के निस्तारण को उनके द्वारा निहित डाटा के वर्गीकरण स्तर के अनुसार नियंत्रित किया जाना चाहिए। डाटा स्टोरेज डिवाइस में बैकअप टेप, हार्ड डिस्क शामिल हैं।
4. सुनिश्चित करें कि किसी भी संवेदनशील डाटा और लाइसेंस प्राप्त सॉफ्टवेयर को हटा दिया गया है या सुरक्षित रूप से अधिलेखित कर दिया गया है जब उपकरण स्थानांतरित या स्क्रैप किया गया है और डाटा सेंटर के

अंदर या बाहर किसी भी उपकरण को लेने से पहले इसे विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा अनुमोदित किया जाना चाहिए. डिवाइस विवरण का अभिलेखीकरण किया जाएगा।

5. बैकअप मीडिया को हटाये (डी.गॉस) और सुरक्षित निस्तारण प्रक्रिया के रूप में टेपों को काट दें।
6. निस्तारण से पूर्व उपकरण से संवेदनशील डाटा और लाइसेंस प्राप्त सॉफ्टवेयर को सुरक्षित रूप से हटा दें।

19. उपकरणों का अनुरक्षण

1. चोरी या क्षति से बचाने के लिए उपकरणों को सुरक्षित स्थानों पर रखा जाना चाहिए।
2. धूल और वायुजनित कणों से होने वाले नुकसान को न्यूनतम करने के लिए सभी उपकरणों को आवधिक अनुरक्षण किया जाना चाहिए।
3. उपकरणों का संचालन वातावरण निर्माता के विनिर्देशों के अनुसार होना चाहिए।
4. विद्युत चुम्बकीय क्षेत्रों, उच्च तापमान, आर्द्रता, विद्युत उतार–चढ़ाव आदि से उपकरणों की सुरक्षा के लिए नियंत्रण होना चाहिए।
5. बाहरी पक्षों द्वारा उपकरणों पर किए गए अनुरक्षण में डाटा को चोरी या रिसाव से बचाने के लिए पर्याप्त नियंत्रण होना चाहिए।
6. सुनिश्चित करें कि यूकेएसडीसी के पास यू.पी.एस., ए.सी. और अग्निशामक आदि निवारक अनुरक्षण के लिए विक्रेता के साथ एस.एल.ए. और अनुबंध है।

20. परिसर से बाहर उपकरणों की सुरक्षा

1. यूकेएसडीसी परिसर और ऑफसाइट स्थान के सभी महत्वपूर्ण उपकरणों को जोखिमों से बचाने के लिए बीमा पॉलिसी के अंतर्गत कवर किया जाना चाहिए।
2. यदि ऑफसाइट स्थान भंडारण आउटसोर्स किया जाता है, तो इन उपकरणों को सुरक्षित रूप से संभालने और बनाए रखने पर बाहरी पक्ष के साथ अनुबंध बनाए रखा जाना चाहिए।
3. आउटसोर्स किए गए ऑफसाइट स्थान पर अनुरक्षित उपकरणों में कुछ बीमा कवर भी होना चाहिए। परिसर से हटाए गए या ऑफसाइट स्थान पर स्थित उपकरण में छेड़छाड़ और डाटा रिसाव से बचाने के लिए पर्याप्त नियंत्रण होना चाहिए।
4. डाटा युक्त सभी वस्तुओं या उपकरणों को डाटा संवेदनशीलता के लिए जांचा जाना चाहिए और उपकरण निस्तारण से पहले सुरक्षित रूप से हटा दिया जाना चाहिए।

21. उपकरणों को हटाना

1. संबंधित कर्मियों द्वारा उपकरण हटाने को अधिकृत किया जाना चाहिए।
2. उपकरण को हटाने का काम करने वाले किसी भी बाहरी पक्ष की पहचान की जानी चाहिए और उसे अधिकृत किया जाना चाहिए।
3. ऑफसाइट पर उपकरण हटाने और मुख्य स्थान पर वापसी दर्ज की जानी चाहिए या ऑफसाइट स्थान पर रसीद दर्ज की जानी चाहिए।

22. अनुपालन

भौतिक और पर्यावरण सुरक्षा नीति में परिभाषित नियंत्रणों के कार्यान्वयन के लिए डाटा सेंटर का प्रभारी प्राथमिक रूप से उत्तरदायी है।

डाटा सेंटर (डाटा सेंटर) के प्रभारी के निम्नलिखित उत्तरदायित्व हैं:–

(क) यह सुनिश्चित करना कि सूचना प्रणालियां सुरक्षित क्षेत्रों में हैं, परिभाषित सुरक्षा परिधियों द्वारा उपयुक्त सुरक्षा अवरोधों और प्रवेश नियंत्रणों द्वारा संरक्षित हैं।

(ख) पर्यावरणीय खतरों से होने वाले नुकसान को रोकने के लिए पर्यावरणीय नियंत्रणों को लागू करके सूचना परिसंपत्तियों की रक्षा करना।

23. प्रयोज्यता

यह नीति यूकेएसडीसी के सभी हितधारकों के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की गई है।

24. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय –8: डाटा सेंटर अभिगम

25. प्रयोजनः

इस नीति का प्रयोजन यूकेएसडीसी डाटा सेंटर में उपकरणों और डाटा की सुरक्षा स्थापित करना है। अवसंरचना, सूचना प्रणाली और डाटा को हमेशा संरक्षित और विश्वसनीय रहना चाहिए। डाटा सेंटर एक्सेस पॉलिसी यूकेएसडीसी की सूचना प्रणालियों तक पहुंचने के लिए आवश्यक दिशा प्रदान करती है।

26. नीति वक्तव्य और उद्देश्यः

यह नीति परिभाषित करेगी कि यूकेएसडीसी के किन सदस्यों या कर्मचारियों, विभागों, ठेकेदारों, या विक्रेताओं आदि को डाटा सेंटर तक पहुंचने की आवश्यकता है, उस पहुंच (एक्सेस) को कैसे नियंत्रित किया जाएगा, और डाटा सेंटर के उपयोग और डाटा सेंटर के भीतर आचरण को नियंत्रित करने वाले नियमों की व्यवस्था करेगी।

27. नियंत्रणः

1. किसी भी डाटा सेंटर तक किसी ऐसे व्यक्ति की पहुंच की अनुमति नहीं है, जिसे स्पष्ट रूप से अनुमति नहीं दी गई है।
2. कार्यालय डाटा सेंटर तक पहुंच और इसकी नियंत्रण प्रक्रियाओं को चिन्हित करेगा और उन्हें परिभाषित करेगा।
3. कार्यालय एक्सेस कंट्रोल मैट्रिक्स में एक्सेस कंट्रोल बनाए रखेगा।
4. अनधिकृत लोगों को महत्वपूर्ण सूचना अवसंरचना की संबंधित सूचना के सभी या किसी भी घटक तक पहुँचने से रोकने हेतु संगठन संरचना में परिवर्तन के अनुसार एक्सेस जोड़ने/हटाने के लिए कार्यालय एक्सेस कंट्रोल मैट्रिक्स की अर्ध–वार्षिक या वार्षिक समीक्षा करेगा।
5. किसी भी डाटा सेंटर तक पहुंच दो–कारक प्रमाणीकरण के माध्यम से होगी, जिसमें कार्ड रीडर या किसी अन्य नवीनतम प्रक्रिया पर भौतिक की–पैड पर एक कुंजी कार्ड और एक पिन इनपुट दोनों की आवश्यकता होगी।
6. डाटा सेंटर के प्रभारी अधिकृत व्यक्तियों का एक रोस्टर बनाए रखेंगे जिन्हें डाटा सेंटरों तक पहुंच की अनुमति है।
7. इस रोस्टर में केवल वे व्यक्ति शामिल होंगे जिन्हें विभागाध्यक्ष या इसके अधिकृत अधिकारी द्वारा अनुमोदित किया गया है, और इस अनुमोदन के बिना किसी को भी प्रवेश की अनुमति नहीं दी जाएगी।
8. डाटा सेंटर तक पहुंच का अनुरोध करने के लिए, विभाग के एक कर्मचारी को अपने पर्यवेक्षक को विभाग के प्रमुख या उसके अधिकृत अधिकारी से अनुमोदन के लिए लिखित रूप में एक अनुरोध प्रस्तुत करना होगा। इस लिखित अनुरोध में निम्न शामिल होंगे:

   (क) व्यक्ति का नाम,

   (ख) व्यक्ति का पद, या विभाग से संबंध,

(ग) व्यक्ति की पहचान संख्या,

(घ) उस व्यक्ति का नाम, पद एवं संपर्क सूचना, जो इस व्यक्ति को एक्सेस देने का अनुरोध कर रहा है,

(ङ) पहुँच की आवश्यकता के कारण का विवरण कि–

(एक) वे कौन सी प्रणाली का अनुरक्षण करेंगे,

(दो) उस अनुरक्षण का स्वरूप,

(तीन) उस अनुरक्षण की महत्वपूर्णता,

9. प्रवेश के लिए मानदंडः प्राधिकृत व्यक्तियों की सूची में केवल निम्नलिखित कारणों से वृद्धि की जाएगी:

(क) व्यक्ति के कार्य की स्थिति के लिए उन्हें आईटी से संबंधित (नेटवर्किंग, सर्वर, स्टोरेज, आदि) हार्डवेयर या सॉफ्टवेयर के रखरखाव की आवश्यकता होती है, जिसे पूरा करने के लिए डाटा सेंटर में भौतिक उपस्थिति की आवश्यकता होती है।

(ख) व्यक्ति के कार्य की स्थिति के लिए उन्हें भौतिक संसाधनों (विद्युत, अग्नि शमन, एयर कंडीशनिंग, आदि) के रखरखाव की आवश्यकता होती है, जिसे पूरा करने के लिए डाटा सेंटर में भौतिक उपस्थिति की आवश्यकता होती है।

10. विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा अनुमोदन पर, डाटा सेंटर के प्रभारी कर्मचारी को अधिकृत व्यक्तियों के रोस्टर में जोड़ देंगे, उस व्यक्ति की कार्ड कुंजी तक उचित पहुंच प्रदान करेंगे, और उस व्यक्ति को प्रवेश के लिए एक अनन्य (यूनिक) पिन जारी करेंगे।

11. डाटा सेंटर के प्रभारी आपातकालीन स्थितियों में उपयोग के लिए डाटा सेंटर की भौतिक कुंजी सम्बन्धी पहुंच बनाए रखेंगे।

28. डाटा सेंटर का अनुश्रवणः

(एक) डाटा सेंटर के प्रभारी डाटा सेंटर तक सभी पहुंच की निगरानी करेंगे और अनधिकृत पहुंच के प्रयासों का उचित प्रत्युत्तर देंगे।

(दो) डाटा सेंटर तक पहुंच की निगरानी के लिए डाटा सेंटर के प्रभारी डाटा सेंटर में कैमरे स्थापित करेंगे और किसी भी आवश्यक जांच में उपयोग के लिए कैमरा फीड रिकॉर्ड करेंगे।

(तीन) यदि अनधिकृत पहुंच का पता चलता है, तो डाटा सेंटर के प्रभारी को सूचना प्रौद्योगिकी विकास एजेंसी (आईटीडीए) विभाग के प्रमुख या उनके अधिकृत अधिकारी को तुरंत सूचित करना चाहिए, ताकि घटना का पता लगाया जा सके और जांच की जा सके।

29. आगंतुकों की पहुंचः

(एक) डाटा सेंटर तक पहुंचने के लिए अधिकृत व्यक्तियों के स्थायी रोस्टर पर कोई भी व्यक्ति अन्य लोगों को डाटा सेंटर तक अस्थायी पहुंच प्रदान करने के लिए भी अधिकृत है यदि यह पहुंच विभाग के व्यवसाय के लिए आवश्यक है। डाटा सेंटर तक पहुंच का अनुरोध करने वाले आगंतुकों (ठेकेदारों, हितधारकों आदि) से पूछताछ विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा संसाधित की जाएगी।

(दो) सभी आगंतुकों की निगरानी एक अधिकृत आईटीडीए कर्मचारी द्वारा की जाएगी जो डाटा सेंटर में पूर्णकालिक रूप से अधिकृत व्यक्तियों की सूची में है।

(तीन) कोई भी अधिकृत व्यक्ति जो किसी भी आगंतुक को डाटा सेंटर अभिगम प्रदान करता है, डाटा सेंटर में रहते हुए आगंतुक के कार्यों हेतु उत्तरदायी होगा।

30. डाटा सेंटर अभिगम नियंत्रणः अभिगम प्राधिकार स्तरः

यूकेएसडीसी डाटा सेंटर एक समेकित सर्वर रूम है जिसका उद्देश्य उच्च स्तर की सुरक्षा की आवश्यकता वाली प्रणालियों हेतु 24X7, 365 दिन उच्च उपलब्धता, सुरक्षित वातावरण प्रदान करना है। डाटा सेंटर तक पहुंच प्राप्त करने के लिए सभी कर्मियों को उचित रूप से प्राधिकार होना चाहिए। आवश्यकतानुसार पहुंच के लिए प्राधिकार करने के कई स्तर हैं। डाटा सेंटर में प्रवेश करते/बाहर निकलते समय सभी व्यक्तियों को लॉग इन किया जाना चाहिए, भले ही उनके प्राधिकार करने का स्तर कुछ भी हो।

(एक) **स्तर III का प्राधिकारः** स्तर III प्राधिकार को यूकेएसडीसी डाटा सेंटर में 24X7, 365 दिन तक बिना सहायता के, बिना मार्गरक्षण के पहुंच प्रदान करता है। डाटा सेंटर में प्रवेश कार्डों को एक्सेस करने की अनुमति दी जाएगी, जो उन व्यक्तियों को सौंपे गए हैं जिन्हें स्तर III का प्राधिकार प्राप्त हुआ है। स्तर III के स्टाफ सदस्य ही एकमात्र ऐसे व्यक्ति हैं जिन्हें डाटा सेंटर स्पेस के भीतर बुनियादी ढांचे में बदलाव (नेटवर्क, कूलिंग, पावर, आदि), उपकरण जोड़ने और/या हटाने, या अचल संपत्ति ऑडिट (इन्वेंट्री) करने के लिए अधिकृत किया गया है। स्तर III का प्राधिकार निम्न को प्रदान किया जाता हैः–

(क) आईटीडीए के अधिकारी;

(ख) डाटा सेंटर प्रबंधक;

(ग) डाटा सेंटर स्टाफ सदस्य;

(घ) डाटा सेंटर तकनीकी टीम और आंतरिक आईटी कर्मचारी जिन्हें विद्युत के वितरण, नेटवर्क कनेक्टिविटी, कूलिंग और डाटा सेंटर के अभिन्यास की देखरेख के लिए नियुक्त किया जाता है।

(ङ) निदेशक, आईटीडीए द्वारा अधिकृत कोई अन्य व्यक्ति, यदि आवश्यक हो।

(दो) **स्तर II का प्राधिकारः** स्तर II के प्राधिकार को यूकेएसडीसी डाटा सेंटर में 24X7, 365 दिन तक बिना सहायता के, बिना मार्गरक्षण के पहुंच प्रदान करता है। डाटा सेंटर में प्रवेश कार्डों को एक्सेस करने की अनुमति दी जाएगी, जो उन व्यक्तियों को सौंपे गए हैं जिन्हें स्तर II का प्राधिकार प्राप्त हुआ है।

(क) आईटीडीए कर्मचारी जिनके पास डाटा सेंटर में रखे गए महत्वपूर्ण सेवाओं के उपकरणों के भौतिक अनुरक्षण तथा मरम्मत हेतु प्राथमिक जिम्मेदारियां हैं।

(ख) स्तर II के स्टाफ सदस्य डाटा सेंटर स्पेस के संबंध में कोई भी परिवर्तन, संशोधन और/या निर्णय लेने के लिए अधिकृत नहीं हैं।

(ग) निदेशक, आईटीडीए द्वारा अधिकृत कोई अन्य व्यक्ति, यदि आवश्यक हो।

(तीन) **स्तर I का प्राधिकारः** स्तर I का प्राधिकार सामान्य कार्यदिवस व्यावसायिक अवधि के दौरान डाटा सेंटर को अनुरक्षण सहायता प्रदान करता है। गैर–व्यावसायिक अवधि के दौरान एक्सेस केस–टू–केस आधार पर प्रदान किया जाएगा। अवधि के बाद की आपात स्थिति में, जो अगले व्यावसायिक दिवस तक प्रतीक्षा नहीं कर सकता, डाटा सेंटर के प्रभारी या नियुक्त डाटा सेंटर कर्मचारियों से संपर्क करके डाटा सेंटर तक आपातकालीन पहुंच

की व्यवस्था की जा सकती है। डाटा सेंटर में प्रवेश उन व्यक्तियों को सौंपे गए कार्ड के द्वारा पहुंच की अनुमति नहीं दी जाएगी, जिन्हें स्तर I का प्राधिकार प्राप्त हुआ है। स्तर I के अधिकृत कर्मियों को हर समय एस्कॉर्ट किया जाना चाहिए, जब तक कि डाटा सेंटर के प्रभारी द्वारा कोई अपवाद नहीं दिया गया हो। स्तर I का प्राधिकार निम्न को प्रदान किया जाता है:

(क) कर्मचारी जो सूचना प्रौद्योगिकी विकास एजेंसी के साथ उनके उपकरणों हेतु एक सुरक्षित स्थान प्रदान करने के लिए अनुबंध करते हैं तथा जिन्हें भौतिक अनुरक्षण और/या मरम्मत कार्यों को करने के लिए कभी–कभी सीधी पहुंच की आवश्यकता होती है।

(ख) अंशकालिक आईटी कर्मचारी (ठेकेदार, आईएसपी, आदि) जो डाटा सेंटर में रखे गए महत्वपूर्ण सेवा उपकरणों के भौतिक अनुरक्षण और मरम्मत के साथ स्तर II/III कर्मचारियों की सहायता करते हैं।

(ग) यदि डाटा सेंटर में उपकरण तक भौतिक पहुंच की आवश्यकता वाली आपात स्थिति किसी अवकाश या प्रशासनिक बंदी के दौरान होती है, तो स्तर I के अधिकार व्यक्ति को डाटा सेंटर तक भौतिक पहुंच प्रदान करने के लिए व्यवस्था की जाएगी। स्तर I के अधिकृत व्यक्तियों को डाटा सेंटर के प्रभारी या अन्य अधिकृत डाटा सेंटर स्टाफ सदस्य से छुट्टी/प्रशासनिक बंदी सम्बन्धी निर्देश प्राप्त होंगे।

(घ) निदेशक, आईटीडीए द्वारा अधिकृत कोई अन्य व्यक्ति, यदि आवश्यक हो।

(चार) **अधिकृत आंतरिक विक्रेता:** अधिकृत आंतरिक विक्रेता सभी आईटीडीए और यूकेएसडीसी कर्मचारी हैं, जो एक संविदात्मक व्यवस्था और उचित अनुमोदन के माध्यम से डाटा सेंटर तक पहुंच रखते हैं। इन कर्मचारियों को सुरक्षा कार्ड एक्सेस दिया भी और नहीं भी दिया जा सकता है। अभिगम स्तर का निर्धारण मामला–दर–मामला आधार पर किया जाएगा। अधिकृत आंतरिक विक्रेताओं में निम्न शामिल हो सकते हैं, लेकिन इन तक सीमित नहीं हैं:

(क) दूरसंचार कर्मचारी

(ख) भौतिक कार्यों से संबंधित कर्मचारी (इलेक्ट्रीशियन, प्लंबर, आदि)

(ग) भवन सेवा कर्मचारी

(पाँच) **अधिकृत बाह्य विक्रेता:** अधिकृत बाह्य विक्रेता सभी आईटीडीए और यूकेएसडीसी के व्यक्ति हैं, जो उचित अनुमोदन के साथ संविदात्मक व्यवस्था के माध्यम से डाटा सेंटर तक पहुंच रखते हैं। बाह्य विक्रेताओं को हमेशा अधिकृत कर्मचारियों द्वारा मार्गरक्षण किया जाना चाहिए।

(छः) **हितधारक:** सभी सरकारी विभागों को हितधारक के रूप में माना जाएगा यदि उस विभाग के सर्वर को यूकेएसडीसी में होस्ट किया गया है।

(सात) **आगंतुक:** आगंतुक वे व्यक्ति हैं जिनके पास स्तर III/II/I या विक्रेता स्तर का प्राधिकार नहीं है। इसमें आईटी कर्मचारी (अंशकालिक और/या पूर्णकालिक) शामिल हो सकते हैं, जिनके पास डाटा सेंटर में रखे गए उपकरणों के अनुरक्षण और मरम्मत की प्रत्यक्ष जिम्मेदारी नहीं है। डाटा सेंटर में आने वाले सभी आगंतुकों को निम्नलिखित दिशानिर्देशों का पालन करना चाहिए:

(क) डाटा सेंटर में प्रवेश करते और बाहर निकलते समय आगंतुकों को लॉग इन और आउट होना चाहिए। आने के उद्देश्य को अभिलिखित किया जाना चाहिए।

(ख) डाटा सेंटर में आगंतुकों के साथ हमेशा एक अधिकृत कर्मचारी होना चाहिए।

(ग) सभी अपवादों को डाटा सेंटर के निदेशक द्वारा प्राधिकृत कार्मिक का अनुमोदन होना चाहिए।

(घ) डाटा सेंटर में सभी मुलाकात कार्यक्रम को कम से कम 24 घंटे पहले डाटा सेंटर के प्रभारी द्वारा निर्धारित किया जाना चाहिए। आपात स्थिति को छोड़कर 24 घंटे के भीतर अनुमति दी जाएगी।

(ङ) भ्रमण समूहों को डाटा सेंटर के आगंतुक माना जाता है, और किसी भी मुलाकात को कम से कम 24 घंटे पहले व्यवस्थित किया जाना चाहिए और विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा अनुमोदित किया जाना चाहिए। भ्रमण समूह एक समय में 15 या उससे कम व्यक्तियों तक सीमित है।

31. अनुपालन

डाटा सेंटर एक्सेस कंट्रोल पॉलिसी में परिभाषित नीति एवं नियंत्रण के कार्यान्वयन हेतु डाटा सेंटर का प्रभारी प्राथमिक रूप से उत्तरदायी है। इस नीति में वर्णित नियंत्रणों को एक सुरक्षित डाटा सेंटर वातावरण बनाए रखने के लिए विकसित किया गया है और डाटा सेंटर में कार्यरत लोगों द्वारा इसका पालन किया जाना चाहिए। यह महत्वपूर्ण है कि कोई भी विभाग/परियोजना जो डाटा सेंटर में अपने एप्लिकेशन, सर्वर आदि की स्थापना पर विचार कर रही है, इन प्रक्रियाओं को पूरी तरह से समझती है और सहमत होती है। डाटा सेंटर में सर्वर तक पहुंच या अनुरक्षण का अनुरोध करने वाले सभी व्यक्तियों को इन प्रक्रियाओं को समझना और उनसे सहमत होना चाहिए।

32. प्रयोज्यता

यह नीति एस.डी.सी. के सभी हितधारकों के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें एस.डी.सी. नेटवर्क तक पहुंच प्रदान की जाती है।

33. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–9 : वर्चुअल प्राइवेट नेटवर्क (वी.पी.एन.)

34. प्रयोजनः

इस नीति का प्रयोजन रिमोट एक्सेस आई.पी.सेक. या एल.2.टी.पी. वर्चुअल प्राइवेट नेटवर्क (वी.पी.एन.) कनेक्शन के लिए दिशानिर्देश प्रदान करना है। वी.पी.एन. सक्षम कनेक्शन का उपयोग करने के लिए संगठन नेटवर्क के लिए रिमोट एक्सेस विशेषाधिकार वाले संगठन के हितधारकों की जिम्मेदारी है।

35. नीतिगत वक्तव्य और उद्देश्यः

यह नीति उन वी.पी.एन.के कार्यान्वयन पर लागू होती है जो एक आई.पी. सेक कॉन्सेंट्रेटर के माध्यम से निर्देशित होते हैं। स्वीकृत कर्मचारी और अधिकृत तृतीय पक्ष (ग्राहक, विक्रेता, आदि) वी.पी.एन.का उपयोग कर सकते हैं, जो केवल सरकारी/संगठन आधिकारिक कार्य के लिए "उपयोगकर्ता प्रबंधित" सेवा है। यूकेएसडीसी में वी.पी.एन. सेवाओं का लाभ उठाने वाले विभागों/संगठनों/निगमों/निदेशालयों के कर्मचारियों को उपयुक्त अनुरोध प्रपत्र भरना चाहिए और यूकेएसडीसी के उपयुक्त प्राधिकारी अर्थात विभागाध्यक्ष या उसके अधिकृत अधिकारी को प्रस्तुत करना चाहिए।

36. नियंत्रणः

1. यह कर्मचारियों की जिम्मेदारी है कि वह अपने वी.पी.एन. क्रेडेंशियल्स को किसी के साथ साझा न करें।
2. वी.पी.एन. के उपयोग को या तो एक बार के पासवर्ड प्रमाणीकरण जैसे टोकन डिवाइस या एक मजबूत पास वाक्यांश के साथ एक सार्वजनिक/निजी कुंजी प्रणाली का उपयोग करके नियंत्रित किया जाना है।
3. जब वी.पी.एन. पर संगठनों के नेटवर्क से जुड़ा होता है, तो संगठन से संबंधित सभी डाटा वी.पी.एन. पर प्रवाहित होंगे और इंटरनेट से संबंधित ट्रैफिक इंटरनेट लिंक के माध्यम से प्रवाहित होगा।
4. वी.पी.एन. गेटवे की स्थापना और प्रबंधन संगठन के संचालन समूहों द्वारा किया जाएगा।
5. वीपीएन, या किसी अन्य तकनीक के माध्यम से आंतरिक नेटवर्क से जुड़े सभी कंप्यूटरों को संगठन के मानक के अनुसार अप–टू–डेट एंटी–वायरस सॉफ़्टवेयर का उपयोग करना चाहिए; इसमें पर्सनल कंप्यूटर शामिल हैं।
6. निष्क्रियता के परिभाषित अंतराल के बाद वी.पी.एन. उपयोगकर्ता स्वचालित रूप से संगठन नेटवर्क (यूकेएसडीसी/स्वान) से डिस्कनेक्ट हो जाएंगे। नेटवर्क से पुनः कनेक्ट करने के लिए उपयोगकर्ता को फिर से लॉग ऑन करना चाहिए।
7. गैर–आईटीडीए स्वामित्व वाले उपकरणों के उपयोगकर्ताओं को संगठन नेटवर्क (यूकेएसडीसी/स्वान), वी.पी.एन. और नेटवर्क नीतियों का अनुपालन करने के लिए उपकरण को विन्यस्त करना होगा।
8. केवल संगठन द्वारा अनुमोदित वी.पी.एन. क्लाइंट का उपयोग किया जा सकता है।
9. व्यक्तिगत उपकरणों के साथ वी.पी.एन. तकनीक का उपयोग करके, उपयोगकर्ता सहमत होते हैं और समझते हैं कि उनकी मशीनें संगठन नेटवर्क का एक वास्तविक विस्तार हैं, और जैसे कि उन्हीं नियमों और विनियमों के

अधीन हैं जो संगठन के स्वामित्व वाले उपकरणों पर लागू होते हैं, अर्थात उनकी मशीनों को संगठन की सूचना सुरक्षा नीतियों के अनुपालन के लिए विन्यस्त किया जाना चाहिए।

37. अनुपालनः

डाटा सेंटर के प्रभारी विभिन्न तरीकों से इस नीति के अनुपालन को सत्यापित करेंगे, जिसमें आवधिक वॉक–थ्रू, वीडियो अनुश्रवण (यदि लागू हो), व्यावसायिक उपकरण रिपोर्ट, आंतरिक और बाहरी ऑडिट और/या निरीक्षण शामिल हैं, लेकिन इन्हीं तक सीमित नहीं है। इस अनुश्रवण के परिणाम उपयुक्त प्राधिकारी को उपलब्ध कराए जाएंगे। इस नीति का उल्लंघन करने वाले कर्मचारी के विरुद्ध अनुशासनात्मक कार्यवाही की जा सकती है, जिसमें रोजगार की समाप्ति तक शामिल है। डाटा सेंटर के प्रभारी निम्नलिखित बातों का ध्यान रखेंगे:

(क) अनुपालन मापनः डाटा सेंटर के प्रभारी विभिन्न तरीकों के माध्यम से इस नीति के अनुपालन को सत्यापित करेंगे, जिसमें आवधिक वॉक–थ्रू, वीडियो अनुश्रवण (यदि लागू हो), व्यावसायिक उपकरण रिपोर्ट, आंतरिक और बाहरी ऑडिट, और वी.पी.एन. नीति समिति को प्रतिक्रिया शामिल है, लेकिन इतनी ही सीमित नहीं है।

(ख) अपवादः नीति के किसी भी अपवाद को निदेशक आईटीडीए द्वारा अनुमोदित किया जाना चाहिए।

38. प्रयोज्यता

यह नीति एस.डी.सी. नेटवर्क से कनेक्ट करने के लिए उपयोग किए जाने वाले कंप्यूटर या वर्कस्टेशन के स्वामित्व वाले या व्यक्तिगत रूप से स्वामित्व वाले संगठन के साथ सभी हितधारकों पर लागू होती है। यह नीति संगठन की ओर से काम करने के लिए उपयोग किए जाने वाले रिमोट एक्सेस कनेक्शन पर लागू होती है, जिसमें ईमेल पढ़ना या भेजना और इंट्रानेट वेब संसाधन देखना शामिल है। इस नीति में संगठन (UKSDC/SWAN) नेटवर्क से जुड़ने के लिए उपयोग किए जाने वाले रिमोट एक्सेस के सभी तकनीकी कार्यान्वयन शामिल हैं।

39. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–10: सर्वर सुरक्षा

40. प्रयोजन:

इस नीति का प्रयोजन यूकेएसडीसी, आईटीडीए के स्वामित्व और/या संचालित आंतरिक सर्वर उपकरण के आधार विन्यास के लिए मानक स्थापित करना है। इस नीति के प्रभावी कार्यान्वयन से आईटीडीए के स्वामित्व वाली सूचना और प्रौद्योगिकी तक अनधिकृत पहुंच कम हो जाएगी।

41. वक्तव्य और उद्देश्य:

यह नीति यूकेएसडीसी., आईटीडीए के स्वामित्व वाले और/या संचालित सर्वर उपकरणों पर और किसी आईटीडीए के स्वामित्व वाले आंतरिक नेटवर्क डोमेन के अर्न्तगत रजिस्ट्रीकृत सर्वरों पर लागू होती है। यह नीति विशेष रूप से आंतरिक नेटवर्क पर उपकरणों के लिए है। डी.एम.जेड. पर बाहरी उपकरणों के सुरक्षित विन्यास के लिए।

42. नियंत्रण:

(एक) स्वामित्व और उत्तरदायित्व

यूकेएसडीसी, आईटीडीए में तैनात सभी आंतरिक सर्वरों का स्वामित्व एक परिचालन समूह के पास होना चाहिए जो डाटा सेंटर के प्रभारी के लिए जिम्मेदार है। व्यावसायिक जरूरतों के आधार पर और विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा अनुमोदित प्रत्येक परिचालन समूह द्वारा स्वीकृत सर्वर कॉन्फिगरेशन गाइड स्थापित और बनाए रखा जाना चाहिए। संचालन समूहों को कॉन्फिगरेशन अनुपालन की निगरानी करनी चाहिए और अपने परिवेश के अनुरूप एक अपवाद नीति लागू करनी चाहिए। प्रत्येक परिचालन समूह को कॉन्फिगरेशन गाइड को बदलने के लिए एक प्रक्रिया स्थापित करनी चाहिए, जिसमें विभाग प्रमुख या उसके अधिकृत अधिकारी द्वारा समीक्षा और अनुमोदन शामिल है।

(क) सर्वर को संगठन उद्यम प्रबंधन प्रणाली के भीतर रजिस्ट्रीकृत होना चाहिए। कम से कम, संपर्क के बिंदु को सकारात्मक रूप से पहचानने के लिए निम्नलिखित सूचना की आवश्यकता है:

1. सर्वर संपर्क और स्थान, और एक बैकअप संपर्क
2. हार्डवेयर और ऑपरेटिंग सिस्टम/संस्करण
3. मुख्य कार्य और अनुप्रयोग, यदि लागू हो

(ख) संगठन उद्यम प्रबंधन प्रणाली में सूचना को अद्यतन रखा जाना चाहिए।

(ग) उत्पादन सर्वरों के लिए कॉन्फिगरेशन परिवर्तनों को विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा उचित परिवर्तन प्रबंधन प्रक्रियाओं और अनुमोदन का पालन करना चाहिए

43. सामान्य विन्यास दिशानिर्देश:

(क) ऑपरेटिंग सिस्टम कॉन्फिगरेशन अनुमोदित आई.एस.एम.एस. दिशानिर्देशों के अनुसार होना चाहिए।

(ख) जिन सेवाओं और अनुप्रयोगों का उपयोग नहीं किया जाएगा, उन्हें जहां व्यावहारिक हो वहां अक्षम कर दिया जाना चाहिए।

(ग) यदि संभव हो तो टी.सी.पी. रैपर्स जैसे एक्सेस–कंट्रोल विधियों के माध्यम से सेवाओं तक पहुंच को लॉग और/या संरक्षित किया जाना चाहिए।

(घ) सिस्टम पर सबसे हालिया सुरक्षा पैच को व्यावहारिक रूप से जल्द से जल्द स्थापित किया जाना चाहिए, तत्काल आवेदन व्यावसायिक आवश्यकताओं में हस्तक्षेप एकमात्र अपवाद है।

(ङ) प्रणालियों के बीच विश्वास संबंध एक सुरक्षा जोखिम हैं, और उनके उपयोग से बचना चाहिए। जब संचार का कोई अन्य तरीका उपयुक्त हो तो विश्वास संबंध का उपयोग न करें।

(च) किसी फंक्शन को करने के लिए हमेशा कम से कम आवश्यक एक्सेस के मानक सुरक्षा सिद्धांतों का उपयोग करें।

(छ) जब एक गैर–विशेषाधिकार प्राप्त खाता करेगा तो रूट का उपयोग न करें।

(ज) यदि सुरक्षित चैनल कनेक्शन के लिए एक कार्यप्रणाली उपलब्ध है (अर्थात, तकनीकी रूप से व्यवहार्य), तो सुरक्षित चैनलों पर विशेषाधिकार प्राप्त पहुंच का प्रदर्शन किया जाना चाहिए, (उदाहरण के लिए एस.एस.एच. या आई.पी. सेक का उपयोग कर एन्क्रिप्टेड नेटवर्क कनेक्शन)।

(झ) सर्वर भौतिक रूप से एक अभिगम–नियंत्रित वातावरण में स्थित होना चाहिए।

(ञ) सर्वरों को विशेष रूप से अनियंत्रित कक्ष क्षेत्रों से संचालित करने से प्रतिबंधित किया गया है।

44. अनुश्रवण

(क) महत्वपूर्ण या संवेदनशील सिस्टम पर सुरक्षा से संबंधित सभी घटनाओं को लॉग किया जाना चाहिए और ऑडिट ट्रेल्स को निम्नानुसार सहेजा जाना चाहिए:

1. सुरक्षा संबंधी सभी लॉग न्यूनतम 24 सप्ताह तक ऑनलाइन रखे जाएंगे।
2. दैनिक वृद्धिशील बैकअप न्यूनतम 6 माह के लिए बनाए रखा जाएगा।
3. लॉग का साप्ताहिक पूर्ण बैकअप न्यूनतम 6 माह के लिए रखा जाएगा।
4. मासिक पूर्ण बैकअप न्यूनतम 2 वर्षों के लिए रखा जाएगा।

(ख) सुरक्षा से संबंधित घटनाओं की रिपोर्ट सर्ट–यूटीके, सी.आई.एस.ओ.(आईटीडीए), एसीएसआईओ (आईटीडीए), एन.सी.आई.आई.पी.सी. और सर्ट–इन को दी जाएगी। अधिकृत अधिकारी (सर्ट–यूटीके/सी.आई.एस.ओ. (आईटीडीए) द्वारा नामित), एन.सी.आई.आई.पी.सी. और सर्ट–इन लॉग की समीक्षा करेंगे और उपयुक्त निकाय को घटनाओं की रिपोर्ट करेंगे (निर्णय सर्ट–यूटीके/सी.आई. एस.ओ. (आईटीडीए) या किसी अन्य प्रासंगिक संगठन द्वारा लिया जाएगा)

(ग) आवश्यकतानुसार सुधारात्मक उपाय निर्धारित किए जाएंगे। सुरक्षा से संबंधित घटनाओं में शामिल हैं, लेकिन इन तक सीमित नहीं हैं:

1. पोर्ट–स्कैन हमले।
2. विशेषाधिकार प्राप्त खातों तक अनधिकृत पहुंच के साक्ष्य।
3. विषम घटनाएँ जो होस्ट पर विशिष्ट अनुप्रयोगों से संबंधित नहीं हैं

45. अनुपालन

(क) आईटीडीए के भीतर अधिकृत संगठनों द्वारा नियमित आधार पर ऑडिट किया जाएगा।

(ख) ऑडिट नीति के अनुसार, ऑडिट का प्रबंधन आंतरिक ऑडिट समूह द्वारा किया जाएगा। आंतरिक लेखा परीक्षा समूह उन निष्कर्षों को फिल्टर करेगा जो किसी विशिष्ट परिचालन समूह से संबंधित नहीं हैं और फिर निष्कर्षों को उपचार या औचित्य के लिए उपयुक्त सहायक कर्मचारियों को प्रस्तुत करेंगे।

(ग) ऑडिट के कारण परिचालन विफलताओं या व्यवधानों को रोकने के लिए हर संभव प्रयास किया जाएगा।

46. प्रयोज्यता

यह नीति यूकेएसडीसी के सभी हितधारकों के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की गई है।

47. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय –11: होस्टिंग वातावरण, आवंटन

48. प्रयोजनः

इस नीति का प्रयोजन विभिन्न राज्य सरकार के विभागों के होस्टिंग दिशानिर्देश प्रदान करना है। यह विभिन्न होस्टिंग विशेषाधिकार वाले संगठन के हितधारकों की जिम्मेदारी है। यूकेएसडीसी में होस्टिंग सेवाओं का लाभ उठाने वाले विभागों/संगठनों/निगमों/निदेशालयों के कर्मचारियों को उचित अनुरोध प्रपत्र भरना चाहिए और विभागाध्यक्ष या उसके अधिकृत अधिकारी के पास जमा करना चाहिए।

49. नीति वक्तव्य और उद्देश्यः

नीति का उद्देश्य राज्य सरकार के विभागों/संगठनों/निगमों/निदेशालयों/सार्वजनिक क्षेत्र की इकाइयों आदि के लिए सुरक्षित और सुरक्षित होस्टिंग वातावरण प्रदान करना है। यह नीति विशेष रूप से यूकेएसडीसी परिसर में होस्टिंग– वातावरण के लिए है।

50. नियंत्रणः

1) उत्तराखंड सरकार के विभागों / संगठनों / निगमों / निदेशालयों / सार्वजनिक क्षेत्र की इकाइयों आदि यूकेएसडीसी में होस्टिंग सेवाओं का लाभ उठाते हैं। उन्हें उपयुक्त अनुरोध प्रपत्र भरना चाहिए और अनुमोदन के लिए संगठन के विभाग प्रमुख या उसके अधिकृत अधिकारी के पास जमा करना चाहिए। आवश्यकता को विभाग के लेटर हेड में साझा किया जाना चाहिए, सक्षम प्राधिकारी द्वारा विधिवत हस्ताक्षरित और मुद्रांकित किया जाना चाहिए।
2) नामांकित समिति (विभाग के प्रमुख या उसके अधिकृत अधिकारी के अधीन) द्वारा प्रस्तुत किए गए अनुरोध के लिए यूकेएसडीसी के भीतर वास्तविक आवंटन पर चर्चा, विश्लेषण और उसे तैयार करेगी।
3) वास्तविक आवंटन अनुरोधित विभागों की सहमति से अनुरोधित आवंटन से कम या उसके बराबर या उससे अधिक हो सकता है।
4) वास्तविक आवंटन निम्नलिखित तकनीकी मानकों पर आधारित होगा जैसे वर्तमान स्थिति, गणना/अतिरिक्त भविष्य की स्थिति (अल्पकालिक और दीर्घकालिक), सुरक्षा अनुपालन, डाटाबेस आकार, डाटा प्रकार, हॉट डाटा और ऑफलाइन डाटा, थ्रूपुट और प्रतिक्रिया समय और बैंडविड्थ।
5) स्वीकृत आवंटन की सूचना अनुरोधकर्ता विभाग/निगमों/निदेशालय आदि को दी जाएगी और अनुरोध की व्यवस्था की जाएगी और उसे पूरा किया जाएगा।
6) यदि विभाग के पास मौजूदा वर्चुअल मशीन हैं और वे उस स्थिति में एस.डी.सी. में प्रव्रजन करना चाहते हैं, तो उन्हें मेमोरी और सी.पी.यू. के पिछले 3 महीने के उपयोग की सूचना देनी होगी।
7) डाटा बेस का लाइसेंस और यदि कोई अन्य लाइसेंस सॉफ्टवेयर है, तो उस स्थिति में विभाग एस.डी.सी. को सॉफ्टवेयर और लाइसेंस प्रदान करेगा।

51. अनुपालनः

इस अभिलेख में वर्णित यह नीति विभिन्न राज्य संगठनों के लिए एक सुरक्षित और सुरक्षित होस्टिंग वातावरण बनाए रखने के लिए विकसित की गई है। डाटा सेंटर में पहुंच का अनुरोध करने वाले सभी व्यक्तियों को इस नीति में पैरामीटर को परिभाषित करने के लिए समझना और सहमत होना चाहिए। सेवा अनुरोध का प्रावधान नीचे दी गई सूची में शामिल होगाः

(क) होस्टिंग वातावरण के लिए अनुरोध,
(ख) अनुरोधित कोर की नई वर्चुअल मशीन बनाएं,
(ग) वर्चुअल मशीन जोड़ें/हटाएं/निकालें,
(घ) वर्चुअल मशीन की मेमोरी बढ़ाएँ/जोड़ें,
(ङ) वर्चुअल मशीन के लिए संग्रहण स्थान बनाएं/जोड़ें/हटाएं/निकालें/घटाएं,
(च) डाटाबेस का अभिलेखीय बैकअप (इंक्रीमेंटल बैकअप/फुल बैकअप),
(छ) स्थानीय बैकअप (इंक्रीमेंटल बैकअप/फुल बैकअप),
(ज) वेब/मोबाइल एप्लिकेशन/पोर्टल होस्ट करना,
(झ) मौजूदा डाटाबेस के साथ एपीआई एकीकरण,
(ञ) सार्वजनिक/निजी आई.पी. उपलब्ध कराना,
(ट) अस्थायी अवधि के लिए होस्ट की गई साइट को अक्षम करना,
(ठ) एस.एम.एस. और ईमेल अधिसूचना अनुरोध।

52. प्रयोज्यता

यह नीति यूकेएसडीसी के सभी हितधारकों के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की गई है।

53. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–12: पैच प्रबंधन

54. प्रयोजन:

इस पैच प्रबंधन नीति का प्रयोजन यूकेएसडीसी को यह सुनिश्चित करने में सक्षम बनाना है कि समुदाय एक डिजिटल संपत्ति को पैच करने के लिए आवश्यक सुरक्षा के बारे में पूरी तरह से जागरूक हो और यूकेएसडीसी डिजिटल संपत्ति को प्रभावित करने वाले सूचना सुरक्षा जोखिमों को कम करने के लिए पैचिंग नियंत्रण और बाधाओं का वर्णन करे।

55. नीति वक्तव्य एवं उद्देश्य:

यूकेएसडीसी की डिजिटल संपत्तियों को सख्त और उचित पैचिंग गतिविधियों द्वारा संरक्षित और सूचीबद्ध किया जाना चाहिए। संवेदनशीलता को पर्याप्त रूप से पैच किया जाना चाहिए। सूचना प्रौद्योगिकी विकास एजेंसी (आईटीडीए) को अपनी संपत्ति की रक्षा करने और उसका अनुपालन सुनिश्चित करने का अधिकार है। पैच प्रबंधन को एक संगठन को सॉफ्टवेयर और इन्फ्रास्ट्रक्चर अपडेट पर नियंत्रण देने के लिए डिज़ाइन किया गया है जिसे वह अभिनियोजित करता है। पैच प्रबंधन प्रक्रिया का उद्देश्य उत्पादन वातावरण में अंतरिम सॉफ्टवेयर और हार्डवेयर रिलीज की तैनाती और रखरखाव को नियंत्रित करना है। प्रभावी पैच प्रबंधन परिचालन दक्षता और प्रभावशीलता बनाए रखता है, सुरक्षा कमजोरियों को दूर करता है, और उत्पादन वातावरण की स्थिरता को बनाए रखता है।

56. नियंत्रण:

पैच प्रबंधन टीम डाटा सेंटर के प्रभारी द्वारा संयुक्त होगी। पैच प्रबंधन प्रक्रिया के लिए निम्नलिखित चरणों का पालन किया जाना चाहिए:

(क) चरण 1: सभी आईटी संपत्तियों की वर्गीकृत सूची बनाएं,
(ख) चरण 2: परीक्षण वातावरण में पैच परिनियोजन का कड़ाई से परीक्षण करें,
(ग) चरण 3: उत्पादन परिवेश में मौजूदा डाटा का बैकअप लें,
(घ) चरण 4: उत्पादन परिवेश में पैच की परिनियोजन को रोल आउट करें,
(ङ) चरण 5: पैच को नियमित रूप से बनाए रखें और मूल्यांकन करें,

57. पैच का सत्यापन

1) यूकेएसडीसी द्वारा उपयोग किए जाने वाले उत्पाद के लिए जब भी कोई नया सुरक्षा पैच जारी किया जाता है, तो प्रक्रिया को लागू किया जाएगा। इसमें ऑपरेटिंग सिस्टम (सर्वर, डेस्कटॉप और लैपटॉप), एप्लिकेशन, डाटाबेस और नेटवर्क और सुरक्षा उपकरण पैच शामिल हैं। यह सुनिश्चित करने के लिए कि सभी पैच ट्रैक किए गए हैं, सिस्टम / नेटवर्क / सुरक्षा प्रशासक को चाहिए:
   1.1 ऑपरेटिंग सिस्टम और अनुप्रयोगों की एक अद्यतन सूची बनाए रखें।
   1.2 विक्रेता की सुरक्षा पैच मेलिंग सूची के लिए सदस्यता लें या नए सुरक्षा पैच प्राप्त करने के लिए विक्रेताओं के साथ अनुबंध करें।

2) प्रशासक जारी किए गए पैच को मान्य करता है यदि यह यूकेएसडीसी पर्यावरण पर परीक्षण वातावरण (यदि उपलब्ध हो) में परीक्षण करके लागू होता है और सी.आई.एस.ओ. और संबंधित एप्लिकेशन मालिकों को पैच के विवरण और परीक्षण परिणामों के बारे में सूचित करता है।

3) व्यवस्थापक को एप्लिकेशन डेवलपर को मूल्यांकन करने और निर्णय लेने के लिए सूचित करना चाहिए कि सर्वर/एप्लिकेशन/डाटाबेस के लिए एक विशिष्ट पैच स्थापित किया जाना है या निम्नलिखित को ध्यान में नहीं रखना है:

3.1 सेवाएं जो पैच को प्रभावित करेंगी,

3.2 परिवर्तन प्रबंधन प्रक्रिया,

3.3 अपेक्षित सिस्टम डाउनटाइम,

4) यदि पैच किसी विशेष सेवा को प्रभावित कर रहा है, जिसका उपयोग यूकेएसडीसी सिस्टम द्वारा नहीं किया जा रहा है, तो इसे खारिज कर दिया जाता है। प्रशासक को उन पैच का रिकॉर्ड रखना चाहिए जो भविष्य के ऑडिट उद्देश्यों के लिए कारणों के साथ स्थापित नहीं किए गए थे।

5) यूकेएसडीसी पर लागू होने वाले पैच के मामले में, प्रशासक को निम्नलिखित विवरणों के साथ पैच रिलीज का रिकॉर्ड रखना चाहिए।

5.1 पैच का नाम,

5.2 प्रभावित सेवा/उत्पाद,

5.3 प्रभावित सर्वर ,

5.4 यूकेएसडीसी के लिए महत्वपूर्ण,

5.5 पैच लागू करने की अंतिम तिथि,

6) क्रांतिकता (क्रिटिकैलिटी) को वर्गीकृत करने के लिए निम्नलिखित दिशानिर्देशों का उपयोग किया जा सकता है: उच्च क्रांतिकता (क्रिटिकैलिटी) (सर्वर):

(क) विक्रेता ने उच्च प्राथमिकता दी है,

(ख) पैच द्वारा संबोधित भेद्यता का दूरस्थ रूप से शोषण किया जा सकता है,

(ग) सार्वजनिक रूप से ज्ञात वर्म्स या ट्रोजन भेद्यता का फायदा उठाते हैं,

(घ) पैच इंटरनेट से सुलभ स्थान पर स्थित सर्वर को प्रभावित करता है,

टिप्पणी: यदि जारी किया गया पैच उपरोक्त श्रेणी के अंतर्गत नहीं आता है, तो इसे कम क्रांतिकता (क्रिटिकैलिटी) के साथ वर्गीकृत किया जाता है।

58. पैच लागू करना

1. डेस्कटॉप/लैपटॉप पैच

1.1 आईटी टीम को एक सैम्पल डेस्कटॉप पर पैच स्थापित करके एक प्रभाव विश्लेषण करना चाहिए।

1.2 यदि पैच लैपटॉप/डेस्कटॉप को प्रभावित नहीं करता है, तो इसे सभी लैपटॉप/डेस्कटॉप पर एक स्वचालित समाधान का उपयोग करके लागू किया जाता है।

2. सर्वर पैच

2.1 एप्लिकेशन डेवलपर को एप्लिकेशन के लिए परीक्षण वातावरण (यदि उपलब्ध हो) में पैच स्थापित करके प्रभाव विश्लेषण करना चाहिए।

2.2 सिस्टम एडमिनिस्ट्रेटर और एप्लिकेशन डेवलपर जांचते हैं कि पैच इंस्टॉलेशन ऑपरेटिंग सिस्टम या टेस्ट सर्वर में एप्लिकेशन की कार्यक्षमता को प्रभावित करता है या नहीं।

2.3 पैच और परिणामों के बारे में विवरण एप्लिकेशन के मालिक को भेजा जाता है।

2.4 एप्लिकेशन डेवलपर को यह तय करने के लिए एप्लिकेशन स्वामी से परामर्श करना चाहिए कि क्या पैच को प्रोडक्शन सर्वर पर स्थापित करने की आवश्यकता है।

2.5 पैच को स्थापित करने के मामले में, परिवर्तन प्रबंधन समिति (सी.एम.सी.) को एक अनुरोध भेजा जाता है।

2.6 अनुमोदन पर, पैच को उत्पादन सर्वर पर मैन्युअल रूप से लागू किया जाता है।

2.7 यदि पैच सिस्टम की कार्यक्षमता को प्रभावित करता है, तो एप्लिकेशन के मालिक को स्थिति के बारे में सूचित किया जाता है।

2.8 सर्वरों की पैचिंग को परिवर्तन प्रबंधन प्रक्रिया का पालन करना चाहिए।

59. ट्रैकिंग परिनियोजन

1) प्रशासकों को सी.आई.एस.ओ. को सिस्टम/उपकरणों पर पैच स्थापना स्थिति के बारे में सूचित करना चाहिए।
2) सभी पैचों के लिए परिनियोजन की स्थिति को कैप्चर करने के लिए प्रशासक को पैच–ट्रैकिंग शीट बनाए रखनी चाहिए।

60. सत्यापन

1) सी.आई.एस.ओ. को तीन महीने में एक बार पैच की स्थापना की समीक्षा करनी चाहिए।
2) सी.आई.एस.ओ., एस.डी.सी. के सूचना सुरक्षा प्रबंधन प्रणाली के दायरे में आने वाले सभी डेस्कटॉप, सर्वर, नेटवर्किंग डिवाइस और सुरक्षा उपकरणों पर भेद्यता मूल्यांकन करने का निर्देश दे सकता है।

61. केन्द्रीकृत पैच प्रबंधन प्रणाली

1) पैच को समय पर लागू करना सुनिश्चित करने के लिए एक सेंटरीकृत पैच प्रबंधन प्रणाली होनी चाहिए।
2) परिनियोजन से पहले पैच का परीक्षण करने की व्यवहार्यता के आधार पर पैच प्रबंधन प्रणाली का उपयोग करके सर्वर, एप्लिकेशन, डाटाबेस और उपकरणों पर पैच लागू करना मैन्युअल या स्वचालित रूप से हो सकता है।

62. पैच अपडेट शेड्यूल ट्रैकिंग

1) माइक्रोसॉफ्ट द्वारा जारी पैच:
   1.1 माह के प्रत्येक दूसरे मंगलवार
2) नेटवर्क और सुरक्षा उपकरणों के विक्रेता द्वारा जारी पैच:
   2.1 जब नई भेद्यता पाई जाती है या उसकी सूचना दी जाती है।
3) यूनिक्स विक्रेता द्वारा जारी पैच:
   3.1 पैच हर 6 महीने में जारी किया जाएगा या जैसे ही एक नई भेद्यता की सूचना दी जाती है, जैसे ही महत्वपूर्ण पैच जारी किया जाता है।

63. अनुपालन

यूकेएसडीसी विभिन्न तरीकों के माध्यम से इस नीति के अनुपालन की पुष्टि करेगा। यूकेएसडीसी पूरे डाटा सेंटर में पैचिंग प्रक्रिया की देखरेख करता है। प्रगति रिपोर्ट और नए पैच रिलीज लगातार वितरित किए जाने चाहिए। एक औपचारिक और अद्यतन संपत्ति सूची।

64. प्रयोज्यता

यह नीति अभिलेख सभी आईटी अवसंरचनाओं, आईटीडीए और यूकेएसडीसी सेवा वितरण के लिए उपयोग किए जाने वाले अनुप्रयोगों पर लागू होता है।

65. प्रवर्तन एवं व्याख्या

(क) इस नीति के उल्लंघन में पाए जाने वाले किसी भी सिस्टम को तत्काल सुधारात्मक कार्यवाही की आवश्यकता होगी। उल्लंघनों को यूकेएसडीसी इश्यू ट्रैकिंग सिस्टम में नोट किया जाएगा और समस्या को दूर करने के लिए सहायता टीमों को भेजा जाएगा। नीति का पालन करने में बार–बार विफल होने पर अनुशासनात्मक कार्रवाई हो सकती है।

(ख) कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–13: परिसंपत्ति प्रबंधन

66. प्रयोजनः

डाटा सेंटर सेवा वितरण में सूचना परिसंपत्ति की रक्षा करना अत्यंत महत्वपूर्ण है और इसलिए, परिसंपत्ति प्रबंधन प्रक्रिया को ठीक से समझना और उसका पालन करना और यह सुनिश्चित करना आवश्यक हो जाता है कि संगठन की सूचना परिसंपत्ति को सभी स्तरों पर पर्याप्त स्तर की सुरक्षा प्रदान की जाती है। इस प्रक्रिया को निम्नलिखित के लिए चरण–दर–चरण कार्यवाही प्रदान करने के लिए तैयार किया गया है:–

(क) संगठन की संपत्तियों की पहचान करना और उनका वर्गीकरण करना;
(ख) एक उपयुक्त प्रारूप में परिसंपत्ति रजिस्टर का संकलन और अनुरक्षण;
(ग) सम्पत्ति की गोपनीयता (सी), अखंडता (आई), और उपलब्धता (ए) रेटिंग का निर्धारण; तथा
(घ) संपत्ति के मालिक, संरक्षक और उपयोगकर्ता की जिम्मेदारियों को समझना; तथा
(ङ) सूचना परिसंपत्ति का उचित वर्गीकरण और पुनर्वर्गीकरण।

67. नीति कथन एवं उद्देश्य

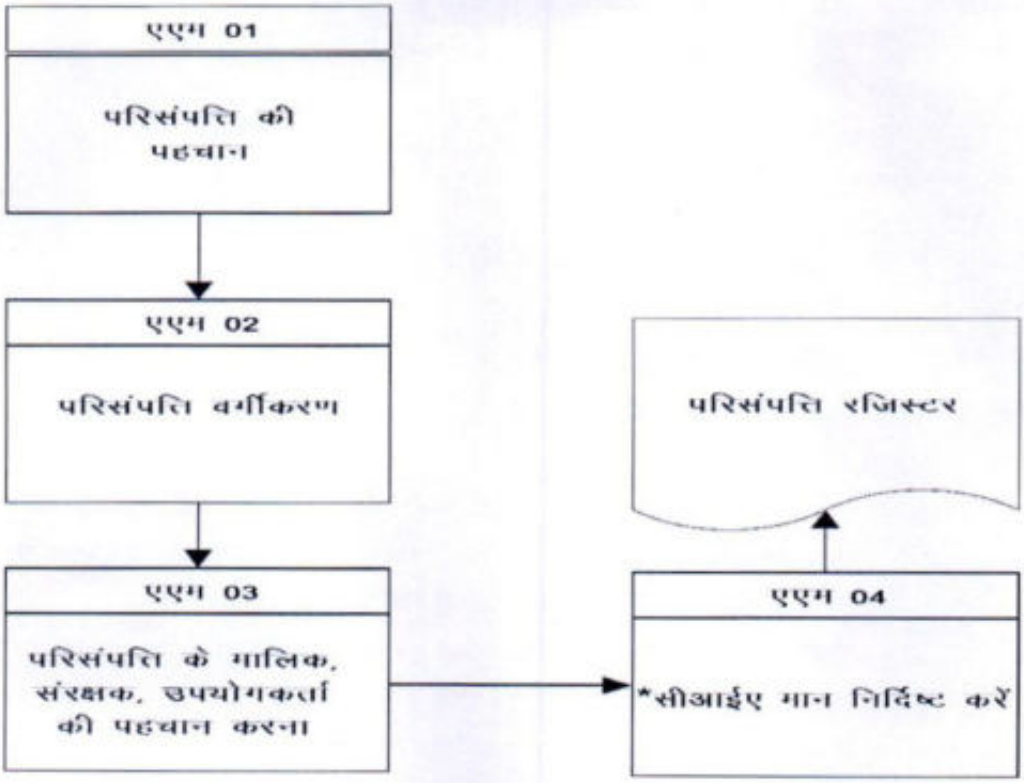
इस नीति अभिलेख का उद्देश्य सभी सूचना परिसंपत्तियों/अवसंरचना परिसंपत्तियों के प्रबंधन हेतु सामान्य दिशानिर्देश प्रदान करना है। नीति का उद्देश्य यूकेएसडीसी में तैनात सूचना और अवसंरचना परिसंपत्तियों की ट्रैकिंग और रिपोर्टिंग के लिए पर्याप्त प्रबंधन नियंत्रण सुनिश्चित करना है।

68. नियंत्रणः

1. परिसंपत्ति प्रबंधन प्रक्रिया

इस प्रक्रिया को चार चरणों में वर्गीकृत किया गया है:–

(क) परिसंपत्ति की पहचान
(ख) परिसंपत्ति वर्गीकरण
(ग) परिसंपत्ति भूमिकाएं और जिम्मेदारियां
(घ) परिसंपत्ति मूल्यांकन



2. संपत्ति की पहचान

(एक) यूकेएसडीसी के भीतर सभी प्रकार की सूचना और आईटी परिसंपत्तियों की पहचान की जाएगी ताकि पर्याप्त सुरक्षा प्रदान की जा सके। सभी सूचना संपत्तियों को निम्नानुसार वर्गीकृत करने की आवश्यकता है:–

(क) सूचना परिसंपत्ति (डिजिटल रूप में): डाटाबेस, उपयोगकर्ता द्वारा उत्पन्न डाटा फाइलें, सिस्टम प्रलेखन, उपयोगकर्ता नियमावली, प्रशिक्षण सामग्री, रन बुक, निरंतरता योजना, आदि।

(ख) सूचना परिसंपत्तियां (गैर–डिजिटल रूप में): सेवा स्तर समझौते (एस.एल.ए.), ग्राहक अनुबंध इत्यादि।

(ग) सॉफ्टवेयर परिसम्पत्तियां: एंटरप्राइज–वाइड एप्लिकेशन सॉफ्टवेयर, सिस्टम सॉफ्टवेयर, सिस्टम डेवलपमेंट एंड एडमिनिस्ट्रेशन टूल्स एंड यूटिलिटीज, ऑपरेटिंग सिस्टम (ओ.एस.)

(घ) हार्डवेयर परिसम्पत्तियां : सर्वर, डेस्कटॉप, लैपटॉप, बैकअप डिवाइस, प्रिंटर आदि।

(ङ) नेटवर्क डिवाइस: स्विच, राउटर, फायरवॉल आदि।

(च) मीडिया उपकरण: सी.डी., डी.वी.डी., यू.एस.बी./जिप ड्राइव, टेप, डी.एल.टी., एल.टी.ओ. आदि।

(छ) लोक परिसंपत्ति: कर्मचारी, अस्थायी कर्मचारी, अनुबंध कर्मचारी आदि।

(ज) सहायक उपयोगिताएँ: संचार सेवाएं, पारेषण लाइनें, बिजली और एच.वी.ए.सी. सिस्टम, इलेक्ट्रॉनिक एक्सेस कंट्रोल सिस्टम, स्मोक डिटेक्शन सिस्टम, आदि।

(दो) सभी सूचना परिसंपत्तियों पर नज़र रखने के लिए एक परिसंपत्ति सूची बनाई जानी चाहिए। संपत्ति प्रबंधक परिसंपत्ति के लिए निम्नलिखित विवरणों की पहचान, कब्जा और अनुरक्षण के लिए जिम्मेदार है:

(क) परिसंपत्ति का शीर्षक,

(ख) परिसंपत्ति आई.डी.,

(ग) परिसंपत्ति का मालिक,

(घ) अभिरक्षक, यदि कोई हो,

(ङ) परिसंपत्ति के उपयोगकर्ता,

(च) बैक–अप विवरण,

3. संपत्ति वर्गीकरण

सूचना को जहां कहीं भी नियत्रिंत या संग्रहीत किया जाता है, उसे अनधिकृत पहुंच, रूपांतरण, प्रकटीकरण और विनाश से उपयुक्त और उचित रूप से संरक्षित करने की आवश्यकता होती है। सभी सूचनाओं को समान महत्व के साथ स्वीकार नहीं किया जाएगा। नतीजतन, सूचना के सापेक्ष मूल्य और संगठन के लिए इसके मूल्य को संरक्षित करने के लिए आवश्यक उचित नियंत्रण के मूल्यांकन के लिए एक रूपरेखा की पहचान करने में मदद करने के लिए श्रेणियों में सूचना का वर्गीकरण आवश्यक है। इस उद्देश्य को प्राप्त करने के लिए, सूचना के निर्माण पर (चाहे डिजिटल या गैर–डिजिटल रूप में), उस सूचना के निर्माता/स्वामी (आमतौर पर सूचना संपत्ति स्वामी) वर्गीकरण के लिए जिम्मेदार होते हैं। इसके अलावा, सूचना संपत्ति का मालिक कम से कम वार्षिक या अविरत आधार पर सूचना के वर्गीकरण की समीक्षा करने के लिए उत्तरदायी है। इस दिशानिर्देश में निर्धारित वर्गीकरण प्रणाली का उद्देश्य सरल और सहज होना है। सार्वजनिक प्रकटीकरण के उद्देश्य से सूचना के अलावा, संगठन की सूचना को निम्नलिखित चार श्रेणियों में से एक में वर्गीकृत किया जाना चाहिए:

(क) **सार्वजनिक:** यह वर्गीकरण उन सूचनाओं पर लागू होता है, जिन्हें जनता के लिए जारी करने के लिए प्राधिकरण द्वारा स्पष्ट रूप से अनुमोदित किया गया है। परिभाषा के अनुसार, इस सूचना का अनाधिकृत प्रकटीकरण जैसी कोई बात नहीं है और इसे संभावित नुकसान के बिना स्वतंत्र रूप से प्रसारित किया जा सकता है। डाटा अखंडता महत्वपूर्ण नहीं है और अनुपलब्धता एक स्वीकार्य जोखिम है। उदाहरण के लिए, सार्वजनिक उपभोग के लिए सृजित सूचना जैसे सार्वजनिक बुलेटिन, नोटिस आदि।

(ख) **आंतरिक:** डाटा जिसका अनाधिकृत प्रकटीकरण नीति के विरुद्ध है, लेकिन उसके कर्मचारियों/विभिन्न राज्य विभागों पर गंभीर या प्रतिकूल प्रभाव पड़ने की उम्मीद नहीं है, उदाहरण के लिए प्रशिक्षण सामग्री, और नीति नियमावली आदि।

(ग) **गोपनीय:** यह वर्गीकरण संवेदनशील व्यावसायिक सूचना पर लागू होता है, जिसका उद्देश्य ई–गवर्नमेंट सेवा वितरण के भीतर उपयोग करना है। संपत्ति की अनधिकृत बाहरी/आंतरिक पहुंच ई–गवर्नमेंट और/या उनके डाटा को होस्ट करने वाले विभागों को प्रभावित करेगी। प्रवेश प्रतिबंधित किया जाना चाहिए। उदाहरण के लिए, विभागीय सूचना, कार्मिक रिकॉर्ड, महत्वपूर्ण परिचालन संबंधी सूचना।

(घ) **प्रतिबंधित:** यह वर्गीकरण सबसे संवेदनशील व्यावसायिक सूचना पर लागू होता है, जो सख्ती से ई–गवर्नेंस सेवा वितरण के भीतर उपयोग के लिए अभिप्रेत है। इसका अनाधिकृत प्रकटीकरण ई–गवर्नेंस सेवा वितरण और इसके ग्राहकों को गंभीरता से और प्रतिकूल रूप से प्रभावित कर सकता है, जिससे कानूनी और वित्तीय प्रभाव और प्रतिकूल जनमत हो सकता है। उदाहरण के लिए, राज्य व्यापार योजनाएँ, मौजूदा अभियोग योजना, विभागीय डाटा, सूचना सुरक्षा डाटा, सरकारी रणनीति अभिलेख आदि।

4. संपत्ति रजिस्टर बनाना:

(क) यूकेएसडीसी एक परिसंपत्ति रजिस्टर, सभी सूचना संचार प्रौद्योगिकी (आईसीटी) बुनियादी ढांचे या संबंधित आश्रित बुनियादी ढांचे जैसे हार्डवेयर संसाधन, सॉफ्टवेयर संसाधन (लाइसेंस और कोड), डिजिटल हस्ताक्षर, डिजिटल डाटा और बैकअप संपत्ति आदि की एक सूची, तैयार करेगा।

(ख) परिसंपत्ति रजिस्टर में प्रत्येक प्रविष्टि का मूल्यांकन इसकी कार्यक्षमता, महत्वपूर्णता और संवेदनशीलता, अन्य संपत्तियों के साथ पूरकता की डिग्री, संबद्ध सामाजिक, राजनीतिक और रणनीतिक मूल्य के आधार पर गोपनीयता की डिग्री और उपलब्धता की समय अवधि के आधार पर किया जाएगा।

(ग) मूल्यांकन सीआईए (गोपनीयता, अखंडता और उपलब्धता) मान निर्दिष्ट करेगा, जिसे सामूहिक रूप से सीआईए मूल्य कहा जाता है।

(घ) एक बार परिसंपत्ति रजिस्टर बनाने के बाद उसे बनाए रखना आदेशात्मक और अनिवार्य है। परिसंपत्ति रजिस्टर के अनुरक्षण के लिए एक नोडल अधिकारी होगा।

(ङ) परिवर्तनों पर नज़र रखने के लिए परिसंपत्ति रजिस्टर की अर्ध–वार्षिक या वार्षिक समीक्षा की जाएगी।

(च) किसी भी कर्मचारी को सौंपी गई प्रत्येक संपत्ति पर हस्ताक्षर के साथ उचित रसीद होनी चाहिए।

5. जोखिम विश्लेषण शीट का निर्माण:

(क) यूकेएसडीसी परिसंपत्ति रजिस्टर में परिसंपत्तियों का जोखिम मूल्यांकन करेगा। इन खतरों / कमजोरियों की घटना की संभावना का मूल्यांकन करके खतरों, कमजोरियों और संपत्ति पर उनके प्रभाव की पहचान करने के लिए एक जोखिम मूल्यांकन की आवश्यकता होती है।

(ख) परिसंपत्ति रजिस्टर में परिसंपत्तियों का जोखिम विश्लेषण सीआईए रेटिंग के आधार पर किया जाएगा।

(ग) नए जोखिमों की पहचान करने और मौजूदा जोखिमों की रेटिंग बदलने के लिए जोखिम मूल्यांकन की अर्ध–वार्षिक या वार्षिक समीक्षा की जाएगी।

6. अवर्गीकरण और अवनयन

परिसंपत्तियों के अवर्गीकरण या अवनयन हेतु निम्नलिखित दिशानिर्देशों का पालन किया जा सकता है:

(क) निर्दिष्ट सूचना संपत्ति स्वामी या डाटा सेंटर के प्रभारी, किसी भी समय, सूचना को अ–वर्गीकृत या डाउनग्रेड कर सकते हैं। इसे प्राप्त करने के लिए, डाटा सेंटर के प्रभारी को मूल आलेख पर दिखने वाले वर्गीकरण लेबल को बदलना चाहिए और सभी ज्ञात प्राप्तकर्ताओं, उपयोगकर्ताओं और परिसंपत्तियों को अधिप्राप्ति प्रबंधक (आईटीडीए) को सूचित करना चाहिए।

(ख) जिस दिनांक से गोपनीय सूचना को अवर्गीकृत या अवनयन (down grade) किया जाएगा उसे संवेदनशील सूचना पर दर्शाया जाना चाहिए।

(ग) डाटा सेंटर के प्रभारी, अनुसूचित अवर्गीकरण या अवनयन (down grade) से पहले किसी भी समय, उस अवधि को बढ़ा सकते हैं जब सूचना एक निश्चित वर्गीकरण स्तर पर बनी रहती है।

(घ) यह निर्धारित करने के लिए कि संवेदनशील सूचना को अवर्गीकृत किया जा सकता है या अवनयन (down grade) किया जा सकता है, छह माह में न्यूनतम एक बार, डाटा सेंटर के प्रभारी को उस सूचना को सौंपे गए संवेदनशीलता वर्गीकरण की समीक्षा करनी चाहिए जिसके लिए वे उत्तरदायी हैं।

7. परिसंपत्ति प्रबंधन भूमिकाएं और उत्तरदायित्वः

(क) सूचना संपत्ति स्वामी

डाटा सेंटर के प्रभारी के पास परिसंपत्ति वर्गीकरण योजना और संबंधित दिशा–निर्देशों के आधार पर संपत्ति को वर्गीकृत करने की जिम्मेदारी होती है, अर्थात संपत्ति की गोपनीयता, अखंडता और उपलब्धता के आधार पर। परिसंपत्तियों का वर्गीकरण प्रलेखित किया जाना चाहिए। सभी अभिलेखों पर सख्त संस्करण नियंत्रण होना चाहिए और प्रत्येक परिवर्तन को नए संस्करण के रूप में सहेजा जाना चाहिए।

डाटा सेंटर के प्रभारी को संपत्ति को उचित सुरक्षा प्रदान करने के लिए लागू किए जाने वाले नियंत्रणों की पहचान और अनुमोदन करना चाहिए। सूचना परिसंपत्ति का स्वामी सूचना संपत्ति की सुरक्षा के लिए जवाबदेह है।

(ख) सूचना संपत्ति अभिरक्षक

सूचना संपत्ति के संरक्षक को संपत्ति की सुरक्षा के लिए और नियंत्रणों को लागू करने (जैसा कि विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा पहचाना और अनुमोदित किया गया है) और यह सुनिश्चित करने के लिए जिम्मेदार होना चाहिए कि वर्गीकृत संपत्तियों के लिए सुरक्षा तंत्र मौजूद हैं।

(ग) सूचना परिसंपत्ति उपयोगकर्ता

चूंकि यूकेएसडीसी सेवा वितरण के दौरान सूचना महत्वपूर्ण और व्यापक है, इसलिए सभी उपयोगकर्ताओं की एक महत्वपूर्ण भूमिका होती है और साथ ही उन्हें सौंपी गई सूचना की सुरक्षा की जिम्मेदारी भी होती है। सभी उपयोगकर्ता जो संवेदनशील सूचना (गैर–सार्वजनिक) के संपर्क में आ

सकते हैं, उनसे अपेक्षा की जाती है कि वे परिसंपत्ति प्रबंधन नीति और इसका समर्थन करने वाले मानकों और दिशानिर्देशों से स्वयं को परिचित करें और इसका लगातार उपयोग करें।

8. सूचना प्रौद्योगिकी परिसंपत्ति का निस्तारण

सूचना प्रणाली तथा परिसंपत्ति का निस्तारण विभाग प्रमुख या उसके अधिकृत अधिकारी के अनुमोदन के बाद उत्तराखंड सरकार के नियमों के अनुसार आईटी परिसंपत्तियों के निस्तारण हेतु तथा इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय और उत्तराखण्ड शासन के नियमों द्वारा परिभाषित किसी भी अन्य नियमों के अनुसार किया जाता है।

69. अनुपालन

(क) डाटा सेंटर का प्रभारी मुख्य रूप से परिसंपत्ति प्रबंधन नीति में परिभाषित नियंत्रणों के कार्यान्वयन के लिए जिम्मेदार है। डाटा सेंटर के प्रभारी की निम्नलिखित जिम्मेदारियां हैं:

(ख) यह सुनिश्चित करने के लिए कि सभी संपत्तियों को ठीक से सूचीबद्ध और मॉनिटर किया गया है।

(ग) सभी संपत्तियों की अद्यतन सूची को प्रोक्योरमेंट मैनेजर (आईटीडीए) को भेजने के लिए।

70. प्रयोज्यता

यह नीति यूकेएसडीसी डाटा सेंटर के संचालन के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी डाटा सेंटर तक पहुंच प्रदान की जाती है।

71. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–14: बैकअप और पुनर्स्थापना

72. प्रयोजनः

यह नीति संगठन में डाटा की सुरक्षा के लिए और डाटा की हानि को रोकने के लिए और आईटी संसाधनों और व्यावसायिक प्रक्रियाओं की बहाली को सुविधाजनक बनाने के लिए यूकेएसडीसी आईटी संसाधनों की डाटा अखंडता और उपलब्धता बनाए रखने के लिए डिज़ाइन की गई है। सुनिश्चित करें कि यह खोये नहीं और उपकरण की विफलता, डाटा के जानबूझकर विनाश, या आपदा की स्थिति में पुनर्प्राप्त किया जा सके।

ई–गवर्नेंस सेवा वितरण में सिस्टम और उपयोगकर्ता डाटा की सुरक्षा करना अत्यंत महत्वपूर्ण है और इसलिए, बैकअप और पुनर्स्थापना प्रक्रियाओं को औपचारिक रूप देना आवश्यक हो जाता है। बैकअप और पुनर्स्थापना प्रक्रिया निम्नलिखित का कार्यान्वयन प्रदान करती है:

(क) सूचना प्रणाली बैकअप की आवृत्ति और वैकल्पिक भंडारण साइटों (यदि ऐसा निर्दिष्ट है) के लिए बैकअप सूचना की स्थानांतरण दर पुनर्प्राप्ति समय उद्देश्यों (आर.टी.ओ.) और पुनर्प्राप्ति बिंदु उद्देश्यों (आर.पी.ओ.) के अनुरूप है।

(ख) जबकि सिस्टम बैकअप सूचना के लिए अखंडता और उपलब्धता प्राथमिक चिंताएं हैं, बैकअप सूचना को अनधिकृत प्रकटीकरण से बचाना भी एक महत्वपूर्ण विचार है जो बैकअप मीडिया में मौजूद सूचना के प्रकार पर निर्भर करता है।

73. नीति कथन और उद्देश्यः

(एक) अभिलेख प्रक्रिया एस.डी.सी. से सेवा वितरण ढांचे में सभी बैकअप पर लागू होती है। इसलिए एस.डी.सी. (यदि लागू हो) में बैकअप नीति के कार्यान्वयन के लिए विस्तृत अनुशंसित प्रक्रियाएं/और टेम्पलेट/ प्रदान करता है।

इसमें निम्नलिखित शामिल हैं:

(क) डाटा सेंटर में सभी महत्वपूर्ण प्रणालियों के लिए बैकअप अनुसूची का निर्माण।
(ख) यह सुनिश्चित करना कि बैकअप नियमित रूप से लिए गए हैं, और एक समीक्षा चक्र को परिभाषित करना।
(ग) विभिन्न प्रणालियों के बैकअप हेतु दिशानिर्देश।
(घ) टेप लेबलिंग योजना।
(ङ) ऑफसाइट संग्रहण।

(दो) इस नीति अभिलेख का प्राथमिक उद्देश्य बैकअप नीति के कार्यान्वयन के लिए निम्नानुसार मार्गदर्शन प्रदान करना है:

(क) बैकअप को इस तरीके से निष्पादित किया जाना चाहिए कि सूचना पुनर्प्राप्ति बिंदु उद्देश्य आर.पी.ओ (recovery point objectives) का समर्थन करे।
(ख) बैकअप की एक सूची बनाए रखा जाना चाहिए।

(ग) परिभाषित आर.पी.ओ. (recovery point objectives) और आर.टी.ओ. (recovery time objectives) को मान्य करने के लिए समय–समय पर बैकअप पुनर्स्थापना की जानी चाहिए।

(घ) बैकअप प्रतिधारण समिति के अनुसार होना चाहिए (जो विभाग के प्रमुख या उसके अधिकृत अधिकारी द्वारा मिलकर बनी हो)।

74. नियंत्रण:

बैकअप

1. बैकअप नियमित रूप से लिया जाना चाहिए ताकि यह सुनिश्चित किया जा सके कि आवश्यकता पड़ने पर डाटा को पुनर्प्राप्त किया जा सकेगा।
2. जिन घटकों का बैकअप लेने की आवश्यकता है, उन्हें एप्लिकेशन स्वामी द्वारा प्रत्येक एप्लिकेशन के लिए परिभाषित किया जाना चाहिए।
3. बैकअप शेड्यूलिंग यह सुनिश्चित करने के लिए किया जाना चाहिए कि सिस्टम संचालन को प्रभावित किए बिना सभी महत्वपूर्ण डाटा का बैक अप लिया गया है।
4. सभी ऑपरेटिंग सिस्टम और एप्लिकेशन सॉफ़्टवेयर के लिए मूल डिस्क का एक सेट यह सुनिश्चित करने के लिए बनाए रखा जाना चाहिए कि एक वैध, वायरस–मुक्त बैकअप मौजूद है और किसी भी समय उपयोग के लिए उपलब्ध है।
5. सिस्टम बैकअप में नियमित पूर्ण और वृद्धिशील बैकअप शामिल होंगे।
6. जो व्यक्ति लैपटॉप/डेस्कटॉप का उपयोग करते हैं, वे अपने सिस्टम का बैकअप लेंगे।
7. बैकअप का प्रकार और आवृत्ति और उपयोग किए जाने वाले बैकअप मीडिया के प्रकार का निर्धारण एप्लिकेशन स्वामी/सिस्टम प्रशासक द्वारा निम्नलिखित मापदंडों को ध्यान में रखते हुए किया जाना चाहिए।

   7.1 संव्यवहार की मात्रा,

   7.2 डाटा की गंभीरता,

   7.3 पुनर्प्राप्ति समय बाध्यता,

8. बैकअप डाटा के प्रतिधारण और संग्रह के लिए समय सीमा को एप्लिकेशन स्वामी या सिस्टम व्यवस्थापक द्वारा परिभाषित किया जाना चाहिए। बैकअप प्रतियों की संख्या जिन्हें बनाए रखने की आवश्यकता है, प्रत्येक एप्लिकेशन के लिए स्पष्ट रूप से परिभाषित की जानी चाहिए।
9. एप्लिकेशन स्वामियों से प्राप्त पुष्टि के अनुसार सिस्टम एडमिनिस्ट्रेटर टीम द्वारा प्रोडक्शन सर्वरों का बैकअप बनाए रखा जाएगा। स्टेजिंग और टेस्ट सर्वर के लिए, बैकअप एप्लिकेशन के मालिक द्वारा लिया जाएगा।
10. बैकअप और पुनर्प्राप्ति कार्यों के लिए भूमिकाएं और उत्तरदायित्व स्पष्ट रूप से परिभाषित किए जाने चाहिए।
11. महत्वपूर्ण डाटा के लिए, विभिन्न मीडिया पर बैकअप की कई प्रतियां रखी जानी चाहिए।
12. बैकअप और पुनर्प्राप्ति संचालन को ट्रैक करने के लिए रिकॉर्ड बनाए रखा जाना चाहिए।

13. व्यवसाय पुनर्प्राप्ति योजना को वार्षिक आधार पर तैयार और परीक्षण किया जाना चाहिए।

75. सिस्टम डाटा / रजिस्ट्री बैकअप

सिस्टम बैकअप हार्डवेयर/सॉफ्टवेयर विफलता या भौतिक आपदा की स्थिति में कंप्यूटर सिस्टम की अखंडता को पुनर्स्थापित करने में सक्षम होगा।

(एक) सैंपलिंग आधार पर डाटा और सिस्टम पुनर्प्राप्ति प्रक्रियाओं का बार–बार परीक्षण किया जाना चाहिए। परीक्षणों के बीच की अधिकतम अवधि तीन माह से अधिक नहीं होनी चाहिए। पुनर्प्राप्ति प्रक्रियाओं का परीक्षण यह सुनिश्चित करने के लिए किया जाना चाहिए कि बैकअप डाटा का उपयोग किसी आपात स्थिति या आपदा की स्थिति में डाटा को पुनः स्थापित करने के लिए किया जा सकता है। बैकअप परीक्षण का रिकॉर्ड रखा जाना चाहिए। जहां एक प्राकृतिक डाटा या सिस्टम रिकवरी की आवश्यकता होती है, इसका उपयोग परीक्षण प्रक्रिया में योगदान करने के लिए किया जा सकता है, बशर्ते कि पुनर्प्राप्ति का विवरण दर्ज किया गया हो।

(दो) डाटा की पुनर्स्थापना के लिए पुनर्प्राप्ति प्रक्रियाओं को बनाए रखा जाना चाहिए और अद्यतित होना चाहिए।

(तीन) उपरोक्त से संबंधित अभिलेखों को लेखा परीक्षा उद्देश्यों के लिए प्रबंधित और बनाए रखा जाना चाहिए।

(चार) सभी उपयोगकर्ताओं को यह सुनिश्चित करना चाहिए कि महत्वपूर्ण संगठनात्मक और व्यक्तिगत डाटा एक मान्यता प्राप्त यूकेएसडीसी डाटा सर्वर पर संग्रहीत है, न कि व्यक्तिगत कंप्यूटर या वर्कस्टेशन पर क्योंकि इनका बैकअप नहीं लिया जाता है।

76. डाटा बैकअप अनुसूची:

1) एक माह के लिए एकांतर सप्ताह के दिनों में वृद्धिशील बैकअप लिया जाएगा।
2) सप्ताह के अंतिम एकांतर दिवस में पूरा बैकअप लिया जाएगा।
3) त्रैमासिक पूर्ण बैकअप एक वर्ष तक के लिए उपलब्ध होगा।
4) पूर्ण मासिक बैकअप की एक प्रति एक वर्ष तक के प्रत्येक माह के लिए ली जाएगी।

77. डाटा प्रतिधारण:

1) इंक्रीमेंटल बैकअप एक माह के लिए रखा जाएगा।
2) मासिक पूर्ण बैकअप एक वर्ष के लिए रखा जाएगा।
3) एक त्रैमासिक पूर्ण बैकअप एक वर्ष के लिए रखा जाएगा।
4) वार्षिक पूर्ण बैकअप की एक प्रति एक वर्ष के लिए सुरक्षित रखी जाएगी।

78. सिस्टम का बैकअप

यूकेएसडीसी सिस्टम के लिए बैकअप संगठन के महत्वपूर्ण व्यवसाय और परिचालन प्रणालियों की सुरक्षा के लिए आवश्यक है। सभी बुनियादी ढांचे, व्यवसाय और डाटा सिस्टम के लिए सिस्टम बैकअप लिया जाना चाहिए

ताकि यह सुनिश्चित हो सके कि प्राथमिक प्रणाली के साथ किसी भी समस्या की स्थिति में, व्यापार–महत्वपूर्ण सिस्टम को उचित समय सीमा के भीतर पुनर्स्थापित किया जा सकता है।

79. बैकअप मीडिया की सुरक्षा

1) सभी बैकअप मीडिया को ठीक से लेबल किया जाना चाहिए।
2) अनधिकृत पहुंच को रोकने के लिए बैकअप मीडिया पर महत्वपूर्ण डाटा सुरक्षित किया जाना चाहिए।
3) बैकअप को भौतिक और पर्यावरणीय खतरों के विरूद्ध और निर्माता के विनिर्देशों के अनुसार सुरक्षित किया जाना चाहिए।
4) टेप को अग्निरोधक अलमारियों में संग्रहित किया जाना चाहिए। बैकअप मीडिया तक पहुंच को प्रतिबंधित किया जाना चाहिए।
5) बैकअप मीडिया में डाटा को नष्ट करते समय या बैकअप मीडिया का पुनः उपयोग करते समय पर्याप्त सुरक्षा उपाय किए जाने चाहिए। संदर्भः सूचना हैंडलिंग लेबलिंग निपटान, वर्गीकरण प्रक्रिया
6) बैकअप मीडिया के संचलन को अनुमोदित किया जाना चाहिए, और उसका एक रिकॉर्ड रखा जाना चाहिए।
7) संवेदनशील प्रणालियों की लॉग फाइलों का बैकअप आवधिक रूप से लिया जाएगा।
8) सिस्टम गतिविधियों के लॉग को बनाए रखने के लिए प्रक्रियाएं स्थापित की जाएंगी। संदिग्ध गतिविधियों के संकेत के लिए एक सक्षम स्वतंत्र पार्टी द्वारा ऐसे लॉग की समीक्षा की जाएगी। ऐसे लॉग के लिए उपयुक्त प्रतिधारण अवधि निर्धारित की जाएगी।
9) कंप्यूटर सिस्टम एक्सेस रिकॉर्ड को कम से कम एक वर्ष के लिए हार्ड कॉपी या इलेक्ट्रॉनिक रूप में रखा जाएगा। रिकॉर्ड, जो कानूनी प्रकृति के हैं और किसी भी कानूनी या विनियमन आवश्यकता या आपराधिक व्यवहार की जांच के लिए आवश्यक हैं, उन्हें देश के कानूनों के अनुसार रखा जाएगा।

80. ऑफसाइट बैकअप सुरक्षा

1) महत्वपूर्ण अनुप्रयोगों के लिए, बैकअप की एक प्रति को ऑफसाइट संग्रहित किया जाना चाहिए।
2) ऑफसाइट भंडारण के लिए प्रतिधारण अवधि को परिभाषित किया जाना चाहिए।
3) यह सुनिश्चित करने के लिए पर्याप्त सुरक्षा उपाय किए जाने चाहिए कि मीडिया को सुरक्षित रूप से एक ऑफसाइट स्थान पर ले जाया जाए।
4) मीडिया में अनधिकृत प्रकटीकरण या संशोधन से डाटा की सुरक्षा सुनिश्चित करने के लिए पर्याप्त सुरक्षा उपाय किए जाने चाहिए।

81. बैकअप सॉफ्टवेयर की सुरक्षा

1) बैकअप प्रक्रिया के लिए बैकअप सॉफ्टवेयर का उपयोग किया जाना चाहिए।
2) बैकअप सॉफ्टवेयर और जिस सिस्टम पर यह कार्य करता है, उसकी सुरक्षा के लिए पर्याप्त सुरक्षा उपाय होने चाहिए।
3) बैकअप सॉफ्टवेयर को उत्पादन में अभिनियोजित करने से पहले सुनिश्चित करें कि उस पर आवश्यक परीक्षण किया गया है।

82. मीडिया प्रबंधन

(एक) मीडिया पुस्तकालय प्रबंधन और सुरक्षा के लिए उत्तरदायित्व स्पष्ट रूप से परिभाषित और सौंपे जाने चाहिए।

(दो) संवेदनशील डाटा वाले सभी मीडिया को एक बंद कमरे या कैबिनेट में संग्रहीत किया जाना चाहिए, जो आग प्रतिरोधी और जहरीले रसायनों से मुक्त होना चाहिए।

(तीन) मीडिया लाइब्रेरी (ऑन–साइट और ऑफ–साइट दोनों) तक पहुंच केवल अधिकृत व्यक्तियों तक ही सीमित होगी। लाइब्रेरी में प्रवेश करने के लिए अधिकृत कर्मियों की एक सूची रखी जाएगी।

(चार) संवेदनशील और बैकअप डाटा वाले मीडिया को देश में तीन अलग–अलग भौतिक स्थानों पर संग्रहित किया जाना चाहिए, जहां कुछ घंटों में पहुंचा जा सकता है।

(पाँच) ऑन–साइट और ऑफ–साइट संग्रहीत सभी मीडिया के लिए एक मीडिया प्रबंधन प्रणाली होनी चाहिए।

(छः) सभी इनकमिंग/आउटगोइंग मीडिया अंतरण को प्रबंधन और उपयोगकर्ताओं द्वारा अधिकृत किया जाएगा।

(सात) सभी मीडिया की एक स्वतंत्र भौतिक सूची जांच कम से कम हर छह महीने में की जाएगी।

(आठ) सभी मीडिया में बाहरी मात्रा की पहचान होनी चाहिए। आंतरिक लेबल, जहां उपलब्ध हों, तय किए जाएंगे।

(नौ) यह सुनिश्चित करने के लिए प्रक्रियाएं होनी चाहिए कि लाइब्रेरी से केवल अधिकृत मीडिया को जोड़ने/हटाने की अनुमति है।

मीडिया प्रतिधारण अवधि कानूनी/विनियामक और उपयोगकर्ता की आवश्यकताओं के अनुसार प्रबंधन द्वारा और अनुमोदित की जाएगी।

83. बैकअप डाटा का स्थानांतरण

यदि एप्लिकेशन सॉफ्टवेयर या बैकअप मीडिया प्रकार में कोई परिवर्तन है, तो पहले से बैकअप किए गए डाटा को नए प्रारूप में परिवर्तित किया जाना चाहिए।

84. डाटा पुनर्प्राप्ति और पुनर्स्थापना

नीति अभिलेख का यह खंड यूकेएसडीसी बैकअप से संबंधित डाटा की पुनर्प्राप्ति के लिए नीति की रूपरेखा तैयार करता है। बैकअप को पुनर्स्थापित करने के लिए विभाग के प्रमुख या उसके अधिकृत अधिकारी (आईटीडीए) को एक अनुरोध प्रस्तुत करना होगा, जो कि महत्वपूर्ण पुनर्स्थापना के मामले में, संबंधित विभाग के प्रमुख द्वारा अधिकृत किया जाएगा। डाटा या सिस्टम को पुनर्प्राप्त करने का अनुरोध आईटी सेवा डेस्क को प्रस्तुत किया जाना चाहिए। डाटा या सिस्टम की हानि के बाद अनुरोध जल्द से जल्द संभव समय पर किया जाना चाहिए।

यूकेएसडीसी डाटा या सिस्टम पुनर्स्थापना के लिए अनुरोध दर्ज करने के लिए किसी सदस्य विभाग या व्यक्ति द्वारा देरी के लिए जिम्मेदारी स्वीकार नहीं कर सकता है। डाटा पुनर्स्थापना गतिविधि सदस्य विभागों द्वारा की जाएगी

1) समय–समय पर पुनर्प्राप्ति की जांच कराते रहना चाहिए।
2) पुनर्प्राप्ति परीक्षण की आवृत्ति एप्लिकेशन स्वामी या सिस्टम व्यवस्थापक द्वारा निर्धारित की जानी चाहिए।
3) सभी पुनर्प्राप्ति और पुनर्स्थापना अनुरोधों को विधिवत अनुमोदित किया जाना चाहिए।

85. अनुपालन

बैकअप और पुनर्प्राप्ति प्रक्रिया अभिलेखों को एप्लिकेशन स्वामी या सिस्टम व्यवस्थापक द्वारा बनाया और अनुरक्षित रखा जाना चाहिए। सभी बैकअप और पुनर्प्राप्ति रिकॉर्ड ठीक से बनाए रखा जाना चाहिए।

86. प्रयोज्यता

यह नीति यूकेएसडीसी के स्वामित्व और संचालित सभी उपकरणों और डाटा पर लागू होती है। डाटा सेंटर के प्रभारी नियमित बैकअप करने के लिए एक सदस्य को प्रतिनिधित्व देंगे। प्रत्यायोजित व्यक्ति बैकअप के परीक्षण के लिए एक प्रक्रिया विकसित करेगा और बैकअप से डाटा को पुनर्स्थापित करने की क्षमता का परीक्षण करेगा।

87. प्रवर्तन और व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय –15: लॉग प्रतिधारण

88. प्रयोजनः

कई व्यावसायिक और अनुपालन कारणों से यूकेएसडीसी के लिए एप्लिकेशन और सिस्टम लॉग महत्वपूर्ण हैं, उन्हें सुरक्षित रखने और पर्याप्त रूप से बनाए रखने की आवश्यकता है।

यह नीति यूकेएसडीसी द्वारा प्रबंधित सर्वर और नेटवर्क उपकरणों पर सिस्टम लॉग के लिए प्रतिधारण और विनाश नियमों की पहचान करती है, जिन्हें लॉग फाइल के रूप में भी जाना जाता है। विशिष्ट व्यावसायिक कारणों से या कानूनी आवश्यकताओं को पूरा करने के लिए आईटीडीए के अनन्य उपयोग के लिए लॉग फाइलें संग्रहीत की जाती हैं। लॉग फाइलों को गोपनीय माना जाता है और इस नीति की गोपनीयता आवश्यकताओं के अधीन हैं, और लॉग फाइलों के लिए प्रतिधारण दिशानिर्देशों में अवधारण दिशानिर्देश और उनके व्यावसायिक उपयोग के पूरा होने के बाद नष्ट हो जाते हैं।

89. नीति कथन और उद्देश्यः

कई व्यावसायिक और अनुपालन कारणों से यूकेएसडीसी के लिए एप्लिकेशन और सिस्टम लॉग महत्वपूर्ण हैं, उन्हें पर्याप्त रूप से संग्रहीत और बनाए रखने की आवश्यकता है। सभी लॉग को गोपनीय और संरक्षित डाटा माना जाता है, और यूकेएसडीसी प्रतिधारण अवधि के दौरान अनधिकृत पहुंच को रोकने के लिए सक्रिय उपाय करता है।

90. नियंत्रणः

1. सभी उत्पादन प्रणालियाँ ऑडिट–लॉगिंग सूचना को रिकॉर्ड और बनाए रखेंगी जिसमें निम्नलिखित सूचना शामिल है:
   - (एक) सिस्टम पर की गई गतिविधियाँ।
   - (दो) वह उपयोगकर्ता या इकाई (अर्थात, सिस्टम खाता) जिसने गतिविधि की थी, जिसमें वह प्रणाली भी शामिल है जिससे गतिविधि की गई थी।
   - (तीन) फाइल, एप्लिकेशन, या कोई अन्य ऑब्जेक्ट जिस पर गतिविधि की गई थी।
   - (चार) वह समय जब गतिविधि हुई थी।
   - (पाँच) गतिविधि का परिणाम (उदाहरण के लिए, सफलता या विफलता)।

2. लॉग की जाने वाली विशिष्ट गतिविधियों में कम से कम निम्नलिखित शामिल होने चाहिए:
   - (एक) सूचना (उपयोगकर्ता नाम जैसी प्रमाणीकरण सूचना सहित) बनाई जाती है, पढ़ी जाती है, अद्यतन की जाती है या हटा दी जाती है।
   - (दो) स्वीकृत या आरंभ किए गए नेटवर्क कनेक्शन।
   - (तीन) सिस्टम और नेटवर्क के लिए उपयोगकर्ता प्रमाणीकरण और प्राधिकरण।

(चार) एक नया उपयोगकर्ता या समूह जोड़ने सहित, एक्सेस अधिकारों को प्रदान करना, संशोधित करना या रद्द करना; उपयोगकर्ता विशेषाधिकार, फाइल अनुमतियाँ, डाटाबेस ऑब्जेक्ट अनुमतियाँ, फायरवॉल नियम और पासवर्ड बदलना।

(पाँच) सॉफ़्टवेयर इंस्टॉलेशन, पैच, अपडेट या अन्य इंस्टॉल किए गए सॉफ़्टवेयर परिवर्तनों सहित सिस्टम, नेटवर्क, या सेवाओं के कॉन्फ़िगरेशन में परिवर्तन।

(छः) किसी एप्लिकेशन और डिवाइस का स्टार्ट–अप, शटडाउन या पुनरारंभ।

(सात) आवेदन प्रक्रिया निरस्त, विफलता, या असामान्य अंत, विशेष रूप से संसाधन समाप्त होने या संसाधन सीमा या सीमा तक पहुंचने के कारण (जैसे सीपीयू, मेमोरी, नेटवर्क कनेक्शन, नेटवर्क बैंडविड्थ, डिस्क स्थान, या अन्य संसाधन), नेटवर्क सेवाओं की विफलता जैसे कि डी.एच.सी.पी. या डीएनएस, या हार्डवेयर दोष।

(आठ) एक सुरक्षा प्रणाली जैसे घुसपैठ रोकथाम प्रणाली (आई.पी.एस), एंटी–वायरस सिस्टम, या एंटी–स्पाइवेयर सिस्टम से संदिग्ध और/या दुर्भावनापूर्ण गतिविधि का पता लगाना।

3. जब तक तकनीकी रूप से अव्यावहारिक या असंभाव्य न हो, सभी लॉग को एक केन्द्रकृत प्रणाली में एकत्रित किया जाना चाहिए ताकि विभिन्न प्रणालियों में गतिविधियों को समानता, प्रवृत्तियों और व्यापक प्रभावों के लिए सहसंबंधित, विश्लेषण और ट्रैक किया जा सके। लॉग एकत्रीकरण सिस्टम में स्वचालित और समय पर लॉग अंतर्ग्रहण, घटना और विसंगति टैगिंग और चेतावनी, और मैन्युअल समीक्षा की क्षमता होनी चाहिए।

4. लॉग की नियमित रूप से मैन्युअल रूप से समीक्षा की जानी चाहिए:

(एक) उपयोगकर्ताओं, प्रशासकों और सिस्टम ऑपरेटरों की गतिविधियों की कम से कम मासिक आधार पर समीक्षा की जानी चाहिए।

(दो) असामान्य व्यवहार की पहचान करने के लिए कम से कम मासिक आधार पर सिस्टम से संबंधित लॉग की समीक्षा की जानी चाहिए।

5. आउटसोर्स किए गए क्लाउड वातावरण का उपयोग करते समय, लॉग को क्लाउड वातावरण के एक्सेस और उपयोग, संसाधन आवंटन और उपयोग, और परिवर्तनों पर रखा जाना चाहिए। क्लाउड वातावरण में गतिविधियों को करने वाले सभी व्यवस्थापकों और ऑपरेटरों के लिए लॉग रखे जाने चाहिए।

6. सभी सूचना प्रणालियों को नेटवर्क टाइम प्रोटोकॉल (एनटीपी) या इसी तरह की क्षमता को लागू करके अपनी घड़ियों को सिंक्रनाइज़ करना चाहिए। सभी सूचना प्रणालियों को एक ही प्राथमिक समय स्रोत के साथ तालमेल बिठाना चाहिए।

91. लॉग फाइलों तक पहुंच

जबकि इस नीति के अंतर्गत शामिल उपयोग लॉग में व्यक्तिगत रूप से पहचान करने वाली सूचना नहीं होती है, लॉग को यूकेएसडीसी द्वारा गोपनीय डाटा के रूप में वर्गीकृत किया जाता है। इसका कारण यह है कि यूकेएसडीसी के पास अन्य सूचना के संयोजन में उपयोग की जाने वाली लॉग फाइलें हमें किसी सेवा के उपयोग पर विशिष्ट सूचना, जैसे विशिष्ट वेब पेज एक्सेस, को किसी दिए गए व्यक्ति के कंप्यूटर के साथ संबद्ध करने की अनुमति दे सकती हैं। साथ ही, कार्यालय किसी भी डिजिटल सूचना/लॉग को एकत्र करने और मान्य करने के लिए जिम्मेदार है और किसी भी जांच दल के साथ संपर्क के केन्द्रीय बिंदु के रूप में कार्य करता है चाहे वह आंतरिक या बाहरी रूप से हो।

92. लॉग फाइलों का प्रतिधारण

लॉग फाइल अवधारण समय इस खंड में परिभाषित तालिका में निर्दिष्ट हैं। यदि किसी लॉग फाइल में प्रासंगिक सूचना है जो भविष्य के संदर्भ के लिए उपयोगी है, एक लंबित संव्यवहार, या प्रबंधन निर्णय के साक्ष्य के रूप में, इसे बनाए रखा जाना चाहिए। यदि इन उद्देश्यों के लिए एक लॉग फाइल की आवश्यकता होती है, तो इन विशिष्ट लॉग को विभाग के प्रमुख या उसके अधिकृत अधिकारी के अनुमोदन के लिए लॉग को नष्ट करने से पहले इन विशिष्ट लॉग को किसी अन्य केन्द्रीय आईटी स्वामित्व वाली प्रणाली में स्थानांतरित करने की जिम्मेदारी है। अपने अधिकतम अवधारण समय तक पहुंचने के बाद भी)। डिफॉल्ट लॉग अवधारण समय अधिकतम 365 दिन है।

93. लॉग फाइलों का निस्तारण

लॉग फाइलों के प्रतिधारण के अनुसार लॉग फाइलों को नष्ट किया जाना चाहिए। सभी मूल, बैकअप और लॉग की प्रतियां नष्ट कर दी जानी चाहिए। इस कारण से, लॉग फाइलों को हटाने योग्य मीडिया में बैकअप नहीं किया जाना चाहिए और उन्हें केन्द्रीयकृत लॉग सर्वर या मशीन के स्थानीय फाइल सिस्टम पर रहना चाहिए, जिस पर वे उत्पन्न होते हैं। इसके अलावा, कंप्यूटर डिस्क छवियों से लॉग फाइलों को बाहर करने के लिए सावधानी बरती जानी चाहिए। यह नीति लॉग प्रविष्टियों के विपरीत लॉग फाइलों को हटाने की अनुशंसा करती है। लॉग को सबसे विनाशकारी और किफायती रूप से नष्ट किया जाना चाहिए।

94. प्रयोज्यता

यह नीति यूकेएसडीसी द्वारा प्रबंधित सर्वरों और नेटवर्क उपकरणों पर लॉग फाइलों पर लागू होती है।

95. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–16: डाटा हानि रोकथाम (डीएलपी)

96. प्रयोजन:

इस नीति का प्रयोजन संगठनों के लिए दिशानिर्देश प्रदान करना है कि कैसे संगठन डाटा को साझा और संरक्षित कर सकते हैं। डाटा हानि निवारण नीति संगठनों को अनधिकृत डाटा एक्सेस को रोकने और संभावित नुकसान से खुद को बचाने में मदद कर सकती है। एक विशिष्ट डीएलपी नीति में तीन तत्व होते हैं:

स्थान: जहां उक्त नीति लागू की जाएगी,

शर्तें: अनिवार्य रूप से, डाटा हानि को रोकने के लिए नीति जिन मापदंडों को खोजती है,

क्रिया: यदि कोई स्थिति निर्धारित शर्तों को पूरा करती है, तो नुकसान को रोकने के लिए एक कार्यवाही की जाती है,

इन उद्देश्यों के अनुसरण में, संगठन का यह कर्तव्य है कि वह संरक्षित सूचना के नुकसान को सक्रिय रूप से रोकें।

97. नीति कथन और उद्देश्य:

परिनियोजित डाटा हानि निवारण समाधान: सभी विभाग महत्वपूर्ण और गैर–महत्वपूर्ण सूचना अवसंरचना के डाटा हानि से बचने/रोकने के लिए आवश्यक आधारभूत संरचना (आईटी और गैर–आई.टी.) तैयार करेंगे। सभी डाटा भंडारण उपकरणों की पहचान, प्राधिकार और सत्यापन करें और उसी तक पहुंच बनाएं।

(एक) सभी डाटा संग्रहण उपकरणों के लिए सुरक्षित संग्रहण सूची प्रबंधित करें।

(दो) डाटा के अनधिकृत प्रवाह के अनुश्रवण के लिए नेटवर्क अनुश्रवण उपकरण प्रबंधित करें।

(तीन) डाटा और किसी भी महत्वपूर्ण सूचना के हस्तांतरण के लिए आधिकारिक ईमेल आई.डी. के उपयोग को लागू करें।

98. नियंत्रण:

1. **उपयुक्त डाटा स्वामियों की पहचान करें:**
   (क) मुख्य रूप से सुरक्षा के लिए उपयुक्त, उपयुक्त डाटा और ऑपरेटिंग इकाइयों की पहचान करें।
   (ख) अतिरिक्त प्राथमिकता डाटा प्रकारों की पहचान करने के लिए इन डाटा स्वामियों के साथ काम करें। जोखिम कम करने के लिए यह एक पुनरावृत्तीय प्रक्रिया है।
   (ग) इसकी भेद्यता और जोखिम कारकों के अनुसार वर्गीकृत किया गया।
2. **उन सभी स्थानों का पता लगाएँ जहाँ आपके संगठन का संवेदनशील डाटा रहता है:**
   (क) डाटा–एट–रेस्ट, डाटा–इन–यूज़, डाटा–इन मोशन, आर्काइव्ड डाटा, और एन्क्रिप्टेड डाटा पर विचार करें।
   (ख) मानक स्थानों पर विचार करें: नेटवर्क डिवाइस, स्टोरेज, डाटाबेस, फाइल सर्वर, वेब पोर्टल, और अन्य एप्लिकेशन, लैपटॉप, ई–मेल सर्वर (एमटीए या प्रॉक्सी), पीएसटी फाइलें, आदि।

(ग) अन्य स्थानों पर विचार करें: मोबाइल डिवाइस, प्रिंटर, स्कैनर, फैक्स मशीन, कॉपियर, ड्रॉपबॉक्स या एवरनोट, यूएसबी ड्राइव, सीडी/डीवीडी, पेपर कॉपी, आईएम, "मुफ्त" वेबमेल सेवाएं, छात्रों और पूर्व छात्रों के लिए विश्वविद्यालय वेबमेल, एफटीपी जैसे फाइल साझा करने वाले ऐप्स।

3. अपने संवेदनशील डाटा को टैग करें।
4. अनुश्रवण करें और जानें कि संवेदनशील डाटा आमतौर पर कैसे उपयोग किया जाता है और आमतौर पर आपके कार्यबल द्वारा उत्पन्न किया जाता है।
5. निर्धारित करें कि संवेदनशील डाटा कहाँ जाता है।
6. अभिगम नियंत्रण तंत्र को परिभाषित करें।
7. उन लोगों की भूमिकाओं को स्पष्ट रूप से परिभाषित करें जो डाटा हानि की रोकथाम में शामिल होंगे। यह केवल डाटा उपयोग की निगरानी और नियम बनाने के बारे में नहीं है। जिम्मेदारियों को अलग करने से दुरुपयोग को रोकने में मदद मिलती है।
8. शुरुआत में इसे सरल रखें। पता करने के लिए एक विशिष्ट प्रकार का डाटा या जोखिम चुनें। लक्ष्य सबसे महत्वपूर्ण डाटा को सुरक्षित करना और जल्दी से एक औसत दर्जे की जीत हासिल करना है, फिर उस पर निर्माण करना है।
9. सीमा तक वर्कअराउंड का अनुमान लगाएं। यदि ईमेल नियम बड़ी फाइलों को संलग्न होने से रोकते हैं, तो क्या कर्मचारी फाइलों को स्थानांतरित करने के अन्य तरीके खोजेंगे? यह सुनिश्चित करने के लिए कार्यप्रवाहों की जांच करें कि डाटा हानि निवारण नीतियां कर्मचारियों के वैध रूप से अपना कार्य करने के रास्ते में नहीं आती हैं।
10. डाटा उपयोग को ब्लॉक करने से पहले उसकी निगरानी करें। संवेदनशील डाटा हानि की रिपोर्ट करने के लिए पहले डाटा हानि रोकथाम उपकरण सेट करें। सुनिश्चित करें कि डाटा स्थानांतरण को अवरुद्ध करने वाले कोई भी नियम कार्यप्रवाह को बाधित नहीं करेंगे।

99. संवेदनशील डाटा के आसपास अतिरिक्त सुरक्षा आवरण:

(क) सबसे अच्छी घटना प्रतिक्रिया (आईआर) उस घटना के लिए है जिसे घटना बनने से बहुत पहले ही विफल कर दिया गया हो।

(ख) अपनी फाइल अनुमतियों की समीक्षा करें।

अपने बचाव की गहन मुद्रा के हिस्से के रूप में संवेदनशील डाटा के लिए अतिरिक्त एन्क्रिप्शन का उपयोग करने पर विचार करें।

100. प्रयोज्यता

यह नीति उन सभी हितधारकों पर लागू होती है जो यूकेएसडीसी नेटवर्क से जुड़ते हैं।

101. प्रवर्तन एवं व्याख्या

सभी हितधारकों से इस नीति के कार्यान्वयन के संबंध में डाटा सेंटर के साथ सहयोग करने की अपेक्षा की जाती है। कोई भी व्यक्ति जो जानबूझकर इस नीति को लागू करने के उद्देश्य से संगठन द्वारा कार्यान्वित किसी भी उपकरण, पद्धति, या प्रौद्योगिकी को बाधित करने, बाईपास करने, निष्फल या बाधित करने का प्रयास करता है,

रोजगार की समाप्ति, आईटीडीए से निष्कासन या कानूनी कार्यवाही सहित उपयुक्त अनुशासनात्मक और उपचारात्मक कार्रवाइयों के अधीन होगा। कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी. एक्ट, 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–17: लॉगिन सुरक्षा

102. प्रयोजन

इस अभिलेख का प्रयोजन, लॉगिन नीति, उत्तराखंड राज्य डाटा सेंटर सूचना नेटवर्क की सुरक्षा को खतरे में डाले बिना यूकेएसडीसी सूचना नेटवर्क पर मौजूद लॉगिन नामों द्वारा दिए गए एक्सेस अधिकारों को सुरक्षित रखना है।

103. नीति कथन और उद्देश्य

यह नीति उन लॉगिन नामों पर लागू होती है जो उनके धारकों को यूकेएसडीसी डाटा सेंटर के सूचना नेटवर्क तक पहुंचने में सक्षम बनाते हैं, चाहे उनकी गंभीरता, महत्व, संवेदनशीलता, या सूचना नेटवर्क के उस हिस्से की कमी हो जिसके लिए एक्सेस की अनुमति दी गई है।

104. नियंत्रण:

1. यूकेएसडीसी सूचना नेटवर्क तक पहुंच के अधिकार वाले सभी उपयोगकर्ताओं के लिए लॉगिन नाम और पासवर्ड हमेशा अनन्य होने चाहिए।
2. कोई लॉगिन नाम कभी भी सामान्य या साधारण नहीं होना चाहिए (उपयोगकर्ता आईडी, लॉगिन, उपयोगकर्ता नाम, व्यवस्थापक, प्रशासक, आदि)।
3. जबकि व्यक्तिगत लॉगिन नाम अक्सर काम करने वाले सहयोगियों के बीच जाने जाते हैं, उपयोगकर्ताओं के पास उनके लॉगिन नामों से जुड़े पासवर्ड की सुरक्षा और गोपनीयता बनाए रखने के लिए व्यक्तिगत और व्यावसायिक जिम्मेदारी होती है। किसी भी उपयोगकर्ता को अपने पासवर्ड को जानबूझकर उजागर नहीं करना चाहिए या अनजाने में अपने संबंधित पासवर्ड की गोपनीयता की उपेक्षा नहीं करनी चाहिए।
4. सिस्टम प्रशासकों को किसी भी लॉगिन को निष्क्रिय करने के लिए लॉगिंग–इन प्रक्रिया के मापदंडों को सेट करना चाहिए, जिसे लगातार 3 बार और असफल रूप से प्रयास किया गया है। यह उपयोक्ताओं को सिस्टम प्रशासकों से संपर्क करने के लिए बाध्य करता है ताकि वे उस स्थिति की व्याख्या कर सकें जिसके कारण वे अपना पासवर्ड सही ढंग से टाइप करने में तीन बार विफल हुए। यह लॉगिन को चोरी होने या उनके संबंधित पासवर्ड को उजागर होने से भी बचाता है।
5. यूकेएसडीसी सूचना नेटवर्क में सभी असफल लॉग–इन प्रयासों की एक नियमित रूप से निर्धारित रिपोर्ट को सिस्टम प्रशासकों द्वारा तैयार और समीक्षा की जानी चाहिए। यदि लॉग इन करने में बार–बार असफल प्रयासों में कोई नियमित या आदतन पैटर्न दिखाई देता है, तो रिपोर्ट की समीक्षा की जानी चाहिए और आईटीडीए में विभाग के प्रमुख या उसके अधिकृत अधिकारी के साथ चर्चा की जानी चाहिए।
6. सभी लॉगिन नामों की एक नियमित रूप से निर्धारित रिपोर्ट, जिन्होंने यूकेएसडीसी सूचना नेटवर्क को 30 दिनों से अधिक समय तक सफलतापूर्वक एक्सेस नहीं किया है, को सिस्टम प्रशासकों द्वारा तैयार और समीक्षा की जानी चाहिए। इनमें से अधिकांश लॉगिन नामों को यूकेएसडीसी सूचना नेटवर्क तक पहुंचने की आवश्यकता की कमी के कारण रद्द कर दिया जाना चाहिए, जब तक कि लॉगिन नाम स्वामी के प्रबंधन द्वारा इस पहुंच की कमी के लिए एक वैध औचित्य प्रदान नहीं किया गया हो।

7. सिस्टम एडमिनिस्ट्रेटर को लॉगिग–इन प्रक्रिया के मापदंडों को तारक, डॉट्स या किसी अन्य प्रतीक के साथ पासवर्ड छिपाने के लिए सेट करना चाहिए जो पासवर्ड को शोल्डर सर्फर के संपर्क में आने से रोकता है।

8. लॉगिन प्रक्रिया को संभावित हैकर्स को लॉगिन नाम की सही वर्तनी या लॉगिन नाम के बारे में किसी अन्य जानकारी का पता लगाने की अनुमति नहीं देनी चाहिए। उदाहरण के लिए, किसी भी संदेश में यह नहीं लिखा होना चाहिए, "क्षमा करें, आपने लॉगिन नाम के लिए गलत पासवर्ड दर्ज किया है"। अक्सर हैकर्स उन लॉगिन नामों को नहीं जानते हैं जिन्हें वे लक्षित कर रहे हैं, और इस तरह के संदेश से उन्हें एक स्टार्टअप सुराग मिल जाएगा कि उन्हें अपने हैकिंग प्रयास के साथ कहाँ जाना चाहिए।

9. एक सफल लॉग–इन प्रयास के लिए प्रक्रिया में अंतिम सफल और/या असफल लॉग–इन प्रयास का समय और तारीख प्रदर्शित होनी चाहिए। यह उपयोगकर्ताओं को यह जानने की अनुमति देता है कि क्या उनके उपयोगकर्ता नाम और पासवर्ड से दूसरों द्वारा समझौता किया गया है क्योंकि वे पहचान लेंगे कि लॉग इन करने का उनका अंतिम प्रयास कब था।

10. एक लॉग–इन सत्र 30 मिनट की निष्क्रियता के बाद समय समाप्त हो जाना चाहिए जिसके परिणामस्वरूप स्वचालित लॉग–ऑफ हो सकता है जहां इसे वहन किया जा सकता है या उन खातों के लिए लॉक–आउट में जहां लॉग–ऑफ नहीं किया जा सकता है या डाटा की क्षति या हानि हो सकती है।

11. महत्वपूर्ण और संवेदनशील प्रणालियों पर लॉग–इन सत्रों के लिए, निम्नलिखित लागू होता है:

    (क) यदि सिस्टम की प्रकृति ऐसी है कि उपयोगकर्ताओं की लंबी उपस्थिति अनावश्यक है, तो लॉग–इन सत्र का समय होना चाहिए, और उपयोगकर्ता को सिस्टम के आधार पर, लॉग ऑफ करने या सिस्टम एक्सेस बनाए रखने के लिए हर बार याद दिलाया जाना चाहिए।

    (ख) सिस्टम की प्रकृति के बावजूद, एंड–यूजर्स को ओएस के कमांड लाइन प्रॉम्प्ट तक पहुंचने की अनुमति नहीं दी जानी चाहिए।

12. कर्मचारी सेवा समाप्ति प्रक्रिया (इस्तीफा या अन्यथा) में एक साइन–ऑफ भाग शामिल होना चाहिए जहां डाटा सेंटर के प्रभारी कर्मचारी को आईटीडीए द्वारा प्रदान किए गए सभी विशेषाधिकारों/सामग्री के कर्मचारी के हैंडओवर पर हस्ताक्षर करते हैं। इसका तात्पर्य यह है कि आईटीडीए द्वारा कर्मचारी को पूर्व में दिए गए हार्डवेयर, सॉफ्टवेयर और एक्सेस अधिकार आईटीडीए को वापस कर दिए जाने चाहिए। इस हैंडओवर का एक हिस्सा कर्मचारी को दिए गए सभी एक्सेस अधिकारों, खातों और लॉगिन नामों को रद्द करना और अक्षम करना है। यह यूकेएसडीसी और कर्मचारी के बीच अंतिम वित्तीय समझौता होने से पहले होना चाहिए।

105. प्रयोज्यता

यूकेएसडीसी नेटवर्क और इंटरनेट संसाधनों का उपयोग करने वाले सभी हितधारकों की इस नीति का पालन करने की जिम्मेदारी है। सिस्टम एडमिनिस्ट्रेटर और डाटा सेंटर के प्रभारी के पास इस नीति को लागू करने और यह सुनिश्चित करने की जिम्मेदारी है कि इसका पालन किया जा रहा है।

106. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी.एक्ट, 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–18: एंटीवायरस

107. प्रयोजनः

एक वायरस स्व–प्रतिकृति कोड का एक भाग है, जो अक्सर एक दुर्भावनापूर्ण सॉफ़्टवेयर प्रोग्राम होता है, जिसे कंप्यूटर पर जानकारी को नष्ट करने या क्षतिग्रस्त करने के लिए डिज़ाइन किया गया है। कुछ वायरस पुनरुत्पादन के अलावा कोई नुकसान नहीं पहुंचाते हैं, लेकिन एक महत्वपूर्ण संख्या विशेष रूप से डाटा हानि का कारण बनती है या दूसरों को उनकी प्रतियां भेजकर फाइलों की गोपनीयता से समझौता करने के लिए डिज़ाइन की जाती है। वायरस के संभावित स्रोतों में साझा मीडिया जैसे फ़्लॉपी डिस्क या सीडी–रोम, इलेक्ट्रॉनिक मेल (संदेशों से जुड़ी फाइलें शामिल हैं, लेकिन इन्हीं तक सीमित नहीं हैं) और नेटवर्क पर कॉपी किए गए सॉफ़्टवेयर या दस्तावेज़, जैसे कि कैंपस नेटवर्क और इंटरनेट शामिल हैं। वायरस का संक्रमण संगठन के लिए लगभग हमेशा महंगा होता है, चाहे डाटा के नुकसान के माध्यम से (संभवतः स्थायी); सिस्टम को ठीक करने के लिए स्टाफ–समय या महत्वपूर्ण कार्य में देरी। किसी भी सेवा, हस्तक्षेप, या कार्यों को जाति, लिंग, आयु, धर्म और विश्वास, भाषा, संचार, संवेदी हानि, विकलांगता और लैंगिकता से उत्पन्न होने वाली किसी भी आवश्यकता पर विचार करना चाहिए। यह दस्तावेज़ यूकेएसडीसी के भीतर एंटी–वायरस सॉफ़्टवेयर के उपयोग को नियंत्रित करने वाली नीति और प्रक्रिया की व्याख्या करता है। नीति कंप्यूटर वायरस संक्रमण के जोखिम को कम करने और वायरस का सामना करने पर क्या करना है, इस पर मार्गदर्शन और दिशा देती है। यूकेएसडीसी नेटवर्क बनाने वाले सॉफ़्टवेयर और हार्डवेयर आवश्यक संसाधन हैं। कंप्यूटर नेटवर्क कर्मचारियों को रोजमर्रा के कर्तव्यों को पूरा करने में मदद करता है। इसके बिना, महत्वपूर्ण संचार प्रणाली मौजूद नहीं होगी। इस नीति का अनुपालन सुनिश्चित करेगा कि यूकेएसडीसी कंप्यूटर नेटवर्क कंप्यूटर वायरस और संबंधित सुरक्षा जोखिमों से सुरक्षित रहेगा। कंप्यूटर वायरस कंप्यूटर नेटवर्क के लिए काफी जोखिम पैदा करते हैं। वायरस कंप्यूटर नेटवर्क पर सिस्टम को गलत तरीके से चलाने और जानकारी खोने या भ्रष्ट करने का कारण बन सकते हैं। इसके परिणामस्वरूप यूकेएसडीसी के लिए उत्पादकता का नुकसान हो सकता है या कानून का संभावित उल्लंघन हो सकता है।

108. नीति कथन और उद्देश्य

इस एंटीवायरस नीति का उद्देश्य उन सभी नियमित, अनुबंध, और तृतीय–पक्ष आउटसोर्स कर्मचारियों को शिक्षित करना है, जो यूकेएसडीसी के लिए काम करेंगे और यूकेएसडीसी की किसी भी आईटी संपत्ति पर लॉग इन क्रेडेंशियल होंगे। यूकेएसडीसी के पास एक ऐसा कंप्यूटिंग नेटवर्क होना चाहिए जो वायरस मुक्त हो। इस नीति का उद्देश्य उन उपायों पर निर्देश प्रदान करना है जो यूकेएसडीसी के कर्मचारियों द्वारा प्रभावी वायरस का पता लगाने और रोकथाम में मदद करने के लिए किए जाने चाहिए।

109. नियंत्रण

एंटी–वायरस सपोर्ट टीमः

1. संपूर्ण एंटी–वायरस बुनियादी ढांचे के प्रबंधन के लिए एक एंटी–वायरस टीम (एवीटी)/आईटी टीम/समन्वयक होना चाहिए।

(क) इंस्टालेशन

1. यूकेएसडीसी नेटवर्क में सभी विंडोज़ डेस्कटॉप, लैपटॉप और सर्वर मशीनों में एक एंटी–वायरस स्थापित होना चाहिए।
2. एंटी–वायरस एजेंट की स्थापना पासवर्ड से सुरक्षित होनी चाहिए।
3. एंटी–वायरस, एंटी–स्पाइवेयर और एंटी–एडवेयर एजेंटों को अंतिम–उपयोगकर्ताओं द्वारा अक्षम नहीं किया जाना चाहिए।
4. एंटी–वायरस एजेंटों को सप्ताह में कम से कम एक बार पूर्ण सिस्टम स्कैन करने के लिए कॉन्फ़िगर किया जाना चाहिए।
5. एंटी–वायरस एजेंटों को सभी फाइलों का वास्तविक समय स्कैन करने के लिए कॉन्फ़िगर किया जाना चाहिए जब वे एक्सेस, कॉपी या स्थानांतरित हो जाते हैं।
6. फ्लॉपी, सीडी रोम और हटाने योग्य मीडिया को उपकरणों के उपयोग से पहले वायरस के लिए स्कैन किया जाना चाहिए।
7. यदि संक्रमित फ़ाइलों को साफ़ नहीं किया जा सकता है, तो एक एंटी–वायरस एजेंट को संक्रमित फ़ाइलों को क्वारंटाइन करने के लिए कॉन्फ़िगर किया जाना चाहिए।
8. आने वाले/बाहर जाने वाले सभी इंटरनेट ट्रैफ़िक को स्कैन करने के लिए इंटरनेट गेटवे पर एंटी–वायरस स्थापित किया जाना चाहिए।

(ख) एंटीवायरस सिग्नेचर अपडेट

1. विक्रेता द्वारा जारी किए जाते ही नए हस्ताक्षर लागू किए जाने चाहिए। यूकेएसडीसी के एंटी–वायरस एप्लिकेशन आर्किटेक्चर को यह सुनिश्चित करना चाहिए कि नए सिग्नेचर अपडेट विक्रेता द्वारा जारी किए जाने के एक दिन के भीतर सभी मशीनों तक पहुंच जाएं। उपरोक्त उद्देश्य को प्राप्त करने के लिए एंटी–वायरस सर्वरों की संख्या, सर्वर हार्डवेयर साइजिंग और बैंडविड्थ आवश्यकताओं को डिजाइन और कार्यान्वित किया जाना चाहिए।
2. यूकेएसडीसी नेटवर्क से जुड़े सभी सिस्टम को निकटतम सर्वर से स्वचालित अपडेट के लिए कॉन्फ़िगर किया जाना चाहिए।
3. सभी सिस्टम जो यूकेएसडीसी नेटवर्क (मोबाइल उपयोगकर्ता) पर नहीं हैं, को सीधे विक्रेता साइट से हस्ताक्षर अद्यतन करने के लिए कॉन्फ़िगर किया जाना चाहिए।
4. एंटीवायरस और एंटी–स्पाइवेयर/एडवेयर सॉफ़्टवेयर को विक्रेता साइट से नवीनतम हस्ताक्षर पैटर्न प्राप्त करने के लिए शेड्यूल किया जाना चाहिए।

(ग) स्थिति रिपोर्ट

1. एवी टीम/आईटी टीम को समय–समय पर विक्रेता साइट के साथ निम्नलिखित मापदंडों की जांच करनी चाहिए।
   1.1 एंटीवायरस सर्वर पर हस्ताक्षर पैटर्न संख्या,

1.2 एजेंटों पर हस्ताक्षर पैटर्न संख्या,

1.3 एंटी–वायरस एजेंट सॉफ़्टवेयर संस्करण संख्या,

1.4 वायरस परिभाषाएं एक सप्ताह से अधिक पुरानी नहीं होनी चाहिए।

2. ए.वी. टीम/आईटी टीम/समन्वयक को स्पाइवेयर या एडवेयर से किसी भी तरह के संक्रमण के साथ डेस्कटॉप, लैपटॉप और सर्वर की भी जांच करनी चाहिए।

3. एंटी–वायरस टीम/आईटी टीम/समन्वयक को सी.आई.एस.ओ. को एंटी–वायरस/ एंटी–स्पाइवेयर/ एंटी–एडवेयर सुरक्षा की स्थिति पर आवधिक रिपोर्ट प्रस्तुत करनी चाहिए।

3.1 नवीनतम हस्ताक्षर पैटर्न के साथ अद्यतन नहीं किए गए पीसी की संख्या,

3.2 वायरस से प्रभावित शीर्ष 10 मशीनें,

3.3 यूकेएसडीसी नेटवर्क में पाए गए शीर्ष 10 वायरस,

3.4 वायरस/स्पाइवेयर/एडवेयर की पहचान और सफाई का प्रतिशत।

(घ) सर्वर सुरक्षा

1. ऑपरेटिंग सिस्टम और एंटी–वायरस सर्वर पर एप्लिकेशन को सख्त अभिलेख के अनुसार सुरक्षित किया जाना चाहिए।

2. एंटी–वायरस सर्वर तक तार्किक पहुंच केवल अधिकृत कर्मियों तक ही सीमित होनी चाहिए।

3. एंटी–वायरस सर्वरों को केवल अधिकृत कर्मियों तक पहुंच के साथ नियंत्रित भौतिक पहुंच वाले वातावरण में रखा जाना चाहिए।

(ङ) सर्वर अनुश्रवण

1. एंटी–वायरस सर्वर के सिस्टम प्रदर्शन की समय–समय पर निगरानी की जानी चाहिए। निम्नलिखित मानकों के लिए प्रतिदिन प्रदर्शन की निगरानी की जानी चाहिए:

1.1 सी.पी.यू. का उपयोग,

1.2 मेमोरी का उपयोग,

1.3 बैंडविड्थ उपयोग।

2. ऑपरेटिंग सिस्टम और एप्लिकेशन लॉग फाइलों की समय–समय पर निगरानी की जानी चाहिए। लॉग की निगरानी के लिए एंटी–वायरस व्यवस्थापक/सिस्टम व्यवस्थापक जिम्मेदार है। इन लॉग का विश्लेषण साप्ताहिक रूप से किया जाना चाहिए:

(क) बफ़र ओवरफ़्लो प्रयास,

(ख) सेवा प्रयासों से इनकार,

(ग) सेवाओं की शुरुआत और रोक,

(घ) उपयोगकर्ता विशेषाधिकारों का संशोधन।

(च) नई भेद्यताओं को ट्रैक करना:

1. एंटी–वायरस टीम / आईटी टीम / समन्वयक को किसी भी नई भेद्यता पर नज़र रखने के लिए जिम्मेदार होना चाहिए जिससे नेटवर्क पर वर्म या वायरस के हमले हो सकते हैं।
2. ए.वी. टीम/आईटी टीम/समन्वयक को नई भेद्यताओं से जुड़े जोखिमों को कम करने के लिए कदम उठाने चाहिए।

(छ) प्रलेखन

1. ए.वी. टीम / आईटी टीम / समन्वयक को सभी एंटी–वायरस घटकों के साथ–साथ एंटी–स्पाइवेयर और एंटी–एडवेयर की स्थापना, कॉन्फ़िगरेशन और प्रशासन के लिए आवश्यक अद्यतन अभिलेखों का अनुरक्षण करना चाहिए।
2. ए.वी. टीम / आईटी टीम / समन्वयक इन दस्तावेजों को सिस्टम प्रशासकों को वितरित करने के लिए जिम्मेदार है।

(ज) तृतीय–पक्ष पहुंच

1. बाह्य उपयोगकर्ताओं को केवल आई.टी./सी.आई.एस.ओ. के प्रमुख से अनुमोदन के बाद ही लैपटॉप/डेस्कटॉप/पामटॉप को यूकेएसडीसी नेटवर्क से जोड़ने की अनुमति दी जानी चाहिए।
2. यूकेएसडीसी नेटवर्क से थर्ड–पार्टी सिस्टम को कनेक्ट करते समय, यह सुनिश्चित करने के लिए जांच की जानी चाहिए कि सिस्टम वायरस और वर्म्स से मुक्त है, सिस्टम को नवीनतम वायरस पैटर्न, एंटी–स्पाइवेयर / एडवेयर सॉफ़्टवेयर की स्थापना, और नवीनतम सुरक्षा पैच की स्थापना के साथ अद्यतन किया जाता है।

(झ) घटना की रिपोर्टिंग

1. यदि कोई वायरस एंटी–वायरस एजेंट द्वारा साफ नहीं किया जा रहा है या सिस्टम से कोई दुर्भावनापूर्ण प्रोग्राम नहीं हटाया जा रहा है, तो उपयोगकर्ताओं को सिस्टम व्यवस्थापक को रिपोर्ट करनी चाहिए।
2. नेटवर्क में वायरस फैलने की स्थिति में, सिस्टम एडमिनिस्ट्रेटर को तुरंत ए.वी. टीम/आईटी टीम/समन्वयक को सूचित करना चाहिए।

(ञ) परिवर्तन प्रबंधन

एंटी–वायरस एप्लिकेशन और कॉन्फ़िगरेशन सेटिंग्स के संबंध में किसी भी महत्वपूर्ण बदलाव को परिवर्तन प्रबंधन प्रक्रिया का पालन करना चाहिए।

(ट) विक्रेता समर्थन:

सॉफ़्टवेयर उन्नयन और तकनीकी सहायता के लिए विक्रेता के साथ सेवा स्तर के अनुबंधों को बनाए रखा जाना चाहिए।

प्रयोज्यता

यूकेएसडीसी नेटवर्क और इंटरनेट संसाधनों का उपयोग करने वाले सभी हितधारकों की इस नीति का पालन करने की जिम्मेदारी है। सिस्टम एडमिनिस्ट्रेटर और डाटा सेंटर के प्रभारी की जिम्मेदारी है कि वे इस नीति को लागू करें और यह सुनिश्चित करें कि इसका पालन किया जा रहा है।

प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी. एक्ट, 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–19: पासवर्ड

110. प्रयोजन

पासवर्ड कंप्यूटर सुरक्षा का एक महत्वपूर्ण पहलू हैं। वे उपयोगकर्ता खातों के लिए सुरक्षा की अग्रिम पंक्ति हैं। गलत तरीके से चुने गए पासवर्ड के परिणामस्वरूप यूकेएसडीसी संसाधनों का अनधिकृत उपयोग और/या शोषण हो सकता है। पासवर्ड के निर्माण और प्रबंधन के लिए मानक इन जोखिमों को बहुत कम करते हैं। यूकेएसडीसी सिस्टम तक पहुंच रखने वाले सभी हितधारक अपने पासवर्ड चुनने और सुरक्षित करने के लिए, उपयुक्त कदम उठाने के लिए जिम्मेदार हैं, जैसा कि बाद के अनुभागों में नीचे उल्लिखित है।

(क) इस नीति को यूकेएसडीसी के भीतर उपयोग के लिए पासवर्ड आवश्यकताओं को परिभाषित करने के लिए संकलित किया गया है। यह नीति सूचना सुरक्षा के लिए यूकेएसडीसी की प्रतिबद्धता और सुविधा के भीतर जोखिमों को दूर करने के लिए इसके सक्रिय दृष्टिकोण को प्रदर्शित करती है।

(ख) एक संगठन के लिए एक सुरक्षित और नियंत्रित सूचना प्रणाली पर्यावरण संचालित करने के लिए महत्वपूर्ण घटकों में से एक अनुमोदित सुरक्षा तंत्र की तैनाती है जो इसकी सुरक्षा सेवाओं (पहचान और प्रमाणीकरण, अभिगम नियंत्रण, डाटा अखंडता और गोपनीयता) का समर्थन करती है। प्रमुख तंत्रों में से एक पूरे संगठन में एक समान पासवर्ड नीति की परिभाषा और कार्यान्वयन है। यहां परिभाषित पासवर्ड नीति से किसी भी विचलन के लिए विभागाध्यक्ष या उसके अधिकृत अधिकारी के पूर्व लिखित अनुमोदन की आवश्यकता होगी।

111. नीति कथन और उद्देश्य

यह अभिलेख निम्नलिखित उद्देश्यों के साथ पासवर्ड निर्माण और प्रबंधन के लिए स्वीकार्य मानकों का वर्णन करता है:

(क) मजबूत पासवर्ड का सृजन,
(ख) उन पासवर्ड की सुरक्षा,
(ग) पासवर्ड बदलने की आवृत्ति,

इस नीति के दायरे में वे सभी कर्मचारी शामिल हैं जिनके पास यूकेएसडीसी सुविधा में रहने वाले किसी भी सिस्टम पर एक खाता है या उसके लिए उत्तरदायी हैं (या एक्सेस का कोई भी रूप जो पासवर्ड का समर्थन करता है या आवश्यक है), या यूकेएसडीसी नेटवर्क तक पहुंच है, या किसी भी गैर–सार्वजनिक यूकेएसडीसी जानकारी को संग्रहीत करता है। इस अभिलेख में परिभाषित सशक्त पासवर्ड निर्माण आवश्यकताएँ उन सभी प्रणालियों पर लागू होती हैं जिनके पास उन्हें पूर्ण करने की सुविधा है। जहां सिस्टम में पासवर्ड आवश्यकताओं को पूर्ण करने के लिए सुविधाएं नहीं हैं, वहां वैकल्पिक आवश्यकताओं को, केस–दर–केस आधार पर, विभाग के प्रमुख या उनके अधिकृत अधिकारी के पूर्व अनुमोदन के साथ लागू किया जा सकता है।

112. नियंत्रण:

जबकि यह पासवर्ड नीति अभिलेख यूकेएसडीसी के स्वामित्व में है, इसका अनुरक्षण विभाग के प्रमुख या उनके अधिकृत अधिकारी द्वारा किया जाएगा।

113. सर्वर तथा डेस्कटॉप

1. यूकेएसडीसी के सभी सर्वर, डेस्कटॉप और लैपटॉप यूकेएसडीसी डोमेन का हिस्सा होने चाहिए। यूकेएसडीसी नेटवर्क में एक मजबूत डोमेन नीति लागू करके डेस्कटॉप के लिए मजबूत पासवर्ड सुनिश्चित किया जाना चाहिए। पासवर्ड नीति के हिस्से के रूप में निम्नलिखित को लागू किया जाना चाहिए:
   - 1.1 पासवर्ड इतिहास – 5 पासवर्ड,
   - 1.2 अधिकतम पासवर्ड आयु – 45 दिन,
   - 1.3 न्यूनतम पासवर्ड आयु – 0 दिन,
   - 1.4 न्यूनतम पासवर्ड लंबाई – 8 संकेताक्षर,
   - 1.5 पासवर्ड को जटिलता की आवश्यकताओं को पूरा करना चाहिए – सक्षम
2. सभी उपयोगकर्ता डेस्कटॉप/लैपटॉप/सर्वर पर स्क्रीन सेवर पासवर्ड (3 मिनट) सक्षम होना चाहिए।
3. विंडोज़ मशीनें जो यूकेएसडीसी परिभाषित डोमेन का हिस्सा नहीं हैं, उनमें से प्रत्येक के लिए इन व्यक्तिगत मशीनों के लिए एक स्थानीय सुरक्षा नीति परिभाषित होनी चाहिए।
4. गैर–विंडोज (लिनक्स) सिस्टम को उपयोगकर्ता पहुंच के लिए समान मजबूत पासवर्ड नीति का पालन करना चाहिए।
5. उपयोगकर्ता को पहले लॉगऑन पर पासवर्ड बदलने के लिए प्रेरित किया जाना चाहिए।

114. एप्लिकेशन

1. सिस्टम एडमिनिस्ट्रेटर को यह सुनिश्चित करना चाहिए कि यूकेएसडीसी के आईआईएस जैसे जेनेरिक एप्लिकेशन का डिफॉल्ट पासवर्ड एप्लिकेशन संस्थापन के बाद हटा दिया गया है।
2. कस्टम एप्लिकेशन को यह सुनिश्चित करना चाहिए कि एप्लिकेशन उपयोगकर्ता पासवर्ड के लिए जटिलता लागू की गई है।
3. यूकेएसडीसी को यह सुनिश्चित करना चाहिए कि विक्रेताओं से खरीदे गए एप्लिकेशन ने मजबूत पासवर्ड नीतियों को लागू किया है या मजबूत पासवर्ड नीतियों को कॉन्फिगर करने की अनुमति दी है।
4. कस्टम एप्लिकेशन में 5 गलत लॉगिन प्रयासों के बाद खाता लॉकआउट सक्षम होना चाहिए।
5. जब भी संभव हो, इन एप्लिकेशन से भेजे जाने पर पासवर्ड की जानकारी एन्क्रिप्ट की जानी चाहिए।
6. कस्टम एप्लिकेशन का 'फॉरगेट पासवर्ड' मॉडयूल सुरक्षित होना चाहिए।
7. व्यावसायिक आवश्यकता के अनुसार एप्लिकेशन उपयोगकर्ताओं के लिए अधिकतम पासवर्ड आयु 90 दिनों तक निर्धारित की जा सकती है; इसे प्रबंधन द्वारा अनुमोदित किया जाना चाहिए।
8. उपयोगकर्ताओं को पहले लॉगिन पर पासवर्ड बदलने के लिए प्रेरित किया जाना चाहिए।

115. डाटाबेस

1. सिस्टम प्रशासकों को यह सुनिश्चित करना चाहिए कि संस्थापन के बाद डाटाबेस से डिफॉल्ट उपयोगकर्ता नाम और पासवर्ड हटा दिए जाते हैं।
2. डाटाबेस उपयोगकर्ताओं के लिए पासवर्ड जटिलता को लागू किया जाना चाहिए।
3. उपयोगकर्ता क्रेडेंशियल जैसे पासवर्ड को डाटाबेस में एन्क्रिप्टेड संग्रहित किया जाना चाहिए।
4. डाटाबेस से प्रेषित होने पर पासवर्ड जानकारी को एन्क्रिप्ट किया जाना चाहिए।
5. डाटाबेस उपयोगकर्ताओं के लिए अधिकतम पासवर्ड आयु व्यावसायिक आवश्यकता के अनुसार 90 दिनों तक निर्धारित की जा सकती है; इसे प्रबंधन द्वारा अनुमोदित किया जाना चाहिए।

116. नेटवर्क उपकरण

1. सिस्टम व्यवस्थापकों को यह सुनिश्चित करना चाहिए कि सभी नेटवर्क डिवाइस में डिफॉल्ट पासवर्ड हटा दिए गए हैं।
2. नेटवर्क उपकरणों में पासवर्ड एन्क्रिप्शन को चालू किया जाना चाहिए।
3. एसएनएमपी के डिफॉल्ट समुदाय स्ट्रिंग्स को एक मजबूत स्ट्रिंग के साथ प्रतिस्थापित किया जाना चाहिए।
4. नेटवर्क डिवाइस पर पासवर्ड की जटिलता सुनिश्चित की जानी चाहिए।
5. उपकरणों के दूरस्थ व्यवस्थापन के लिए, उपयोगकर्ता नाम और पासवर्ड एक एन्क्रिप्टेड प्रारूप में भेजे जाने चाहिए।

   5.1 नेटवर्क पर प्रसारित होने वाले डाटा को एन्क्रिप्ट करने के लिए उपकरणों पर एस.एस.एच. सक्षम करें।

117. अनुश्रवण

1. सिस्टम प्रशासकों को यह सुनिश्चित करना चाहिए कि चक्रीय पासवर्ड का उपयोग नहीं किया जाता है।
2. प्रशासनिक गतिविधियों के लिए उपयोग किए जाने वाले सभी पासवर्डों को एक पत्र/लिफाफे में प्रलेखित किया जाना चाहिए और निदेशक आईटीडीए को सौंप दिया जाना चाहिए।
   - 2.1 पासवर्ड बदले जाने की स्थिति में इस दस्तावेज़ को अद्यतन किया जाना चाहिए।
   - 2.2 प्रशासनिक पासवर्ड बाहरी ठेकेदारों या विक्रेताओं के सामने प्रकट नहीं किए जाने चाहिए।
   - 2.3 दिन–प्रतिदिन की गतिविधियों के लिए एडमिनिस्ट्रेटर या रूट अकाउंट और पासवर्ड का उपयोग नहीं किया जाना चाहिए।
3. यूकेएसडीसी कंप्यूटर सिस्टम या डिवाइस के सभी असफल लॉगइन प्रयासों को लॉग किया जाना चाहिए।
4. बाहरी ठेकेदारों के लिए दिए गए खातों को कार्य पूरा होने के बाद अक्षम कर दिया जाना चाहिए।
5. पासवर्ड के 5 असफल प्रयासों के बाद उपयोगकर्ता खाता लॉक कर दिया जाना चाहिए।

118. प्रशिक्षण

1. उपयोगकर्ताओं को पासवर्ड का उपयोग करने की सर्वोत्तम प्रथाओं के बारे में प्रशिक्षित किया जाना चाहिए।
2. नए उपयोगकर्ताओं के लिए प्रेरण प्रशिक्षण में यूकेएसडीसी की पासवर्ड नीति शामिल होनी चाहिए।

119. सामान्य दिशानिर्देश

1. पासवर्ड कम से कम 8 अक्षरों का होना चाहिए जिसमें संख्यात्मक और विशेष वर्ण हों। जैसे जटिलता के लिए एक साधारण पासवर्ड जैसे 'security' को $ecuR1tY में बदला जाना चाहिए।
2. पासवर्ड पहले उपयोग किए गए पासवर्ड से अलग होना चाहिए।
3. रिक्त पासवर्ड की अनुमति नहीं होनी चाहिए।
4. पासवर्ड उपयोगकर्ता आईडी/नाम के समान नहीं होना चाहिए।
5. पासवर्ड साझा करना निषिद्ध है।
6. किसी आपात स्थिति के मामले में, उपयोगकर्ताओं को केवल अधिकृत कर्मियों को ही पासवर्ड का खुलासा करना चाहिए – अनुरोध करने वाले व्यक्ति की सकारात्मक पहचान होने के बाद। पासवर्ड इस्तेमाल करने के तुरंत बाद बदल देना चाहिए।
7. जब कोई कर्मचारी संगठन छोड़ देता है, तो उपयोगकर्ता खाता तुरंत अक्षम या हटा दिया जाना चाहिए।
8. किसी समझौता या लीकेज के तुरंत बाद पासवर्ड बदल देना चाहिए।
9. पासवर्ड बनाने के लिए विभिन्न तरीकों का प्रयोग करें ताकि उन्हें याद रखना आसान हो।
   - 9.1 आप किसी कविता या गीत या अपने पसंदीदा वाक्यांश या उद्धरण में से एक या दो पंक्तियाँ चुन सकते हैं और प्रत्येक शब्द के पहले अक्षर का उपयोग कर सकते हैं। उदाहरण के लिए 'thing of beauty is joy forever' tobijf12# बन जाता है।
   - 9.2 पासवर्ड अक्षर संवेदी होते हैं: उपरोक्त उदाहरण का उपयोग किया जाए तो, TobiJF, tobIJF, और tobijF पासवर्ड अलग–अलग हैं और यदि मिश्रित केस पासवर्ड का उपयोग किया जाता है तो पासवर्ड की सुरक्षा बढ़ाई जा सकती है।
   - 9.3 मजबूत पासवर्ड बनाने की एक अन्य रणनीति अक्षरों को संख्याओं या वर्णों से बदलना है। उदाहरण के लिए, tobijf t0b1jf बन जाता है जहाँ अक्षर "o" को अंक "0" से बदल दिया गया है और अक्षर "i" को अंक "1" से बदल दिया गया है।
10. कम से कम दो छोटे असंबंधित शब्द चुनें और उन्हें विशेष प्रतीकों या संख्याओं के साथ जोड़ दें। उदाहरण के लिए, awn, crat, it तीन असंबंधित शब्द हैं जो शब्दों को आपस में जोड़ने पर 'awncratit' बन जाते हैं।
11. पासवर्ड निर्माण उपयोगिता का उपयोग करके प्रशासनिक पासवर्ड बनाया जा सकता है। इस उपयोगिता को संचालन समिति द्वारा अनुमोदित किया जाना चाहिए।

1. एप्लिकेशन विकास मानक:

एप्लिकेशन डेवलपर्स को यह सुनिश्चित करना चाहिए कि उनके प्रोग्राम में निम्नलिखित सुरक्षा सावधानियां शामिल हैं:

(क) अलग–अलग उपयोगकर्ताओं के प्रमाणीकरण का समर्थन करेगा, न कि समूहों का।

(ख) पासवर्ड को स्पष्ट टेक्स्ट में या किसी भी आसानी से प्रतिवर्ती रूप में संग्रहीत नहीं करेगा।

(ग) TACACS+, RADIUS, और/या X.509 को LDAP सुरक्षा पुनर्प्राप्ति के साथ जहां भी संभव हो, समर्थन करेगा।

2. **अभिलेख परिवर्तन प्रबंधनः**

यूकेएसडीसी का मानना है कि यह सुनिश्चित करने के लिए इस पासवर्ड नीति को चालू रखना महत्वपूर्ण है कि यह सुरक्षा मुद्दों को सही ढंग से संबोधित करती है और व्यावसायिक मुद्दों और प्रौद्योगिकियों के विकास के साथ अद्यतित है। यह नीति एक जीवंत अभिलेख है जिसकी वार्षिक रूप से समीक्षा की जाएगी और/या आवश्यकतानुसार अद्यतन किया जाएगा। विभाग के प्रमुख या इसके अधिकृत अधिकारी आवश्यक परिवर्तनों का मसौदा तैयार करेंगे और यूकेएसडीसी की सूचना सुरक्षा संचालन समिति द्वारा उपयुक्त के रूप में उनकी समीक्षा और अनुमोदन करेंगे। विभाग के प्रमुख या उनके अधिकृत अधिकारी और सूचना सुरक्षा कार्यान्वयन समूह के सदस्य यूकेएसडीसी समुदायों को परिवर्तनों के बारे में सूचित करेंगे। यूकेएसडीसी का कोई भी व्यक्ति मौजूदा नीति में संशोधन की आवश्यकता का निर्धारण कर सकता है। इस नीति में परिवर्तन के लिए अनुशंसाओं को विभागाध्यक्ष या उसके अधिकृत अधिकारी को सूचित किया जाना चाहिए।

120. प्रयोज्यता

पासवर्ड नीति उन सभी खातों पर लागू होती है जिनका उपयोग यूकेएसडीसी संसाधनों तक पहुँचने के लिए किया जाता है। कोई भी उपकरण जो इस नीति में उल्लिखित न्यूनतम–सुरक्षा आवश्यकताओं को पूरा नहीं करता है, उसे नेटवर्क से हटाया जा सकता है, अक्षम किया जा सकता है, आदि जब तक कि उपकरण इस नीति मानक का अनुपालन नहीं कर सकता। डाटा सेंटर के प्रभारी इस नीति के अनुपालन को सुनिश्चित करने के लिए आंतरिक नीतियों, प्रथाओं आदि को लागू करने, समीक्षा करने और निगरानी करने के लिए जिम्मेदार हैं। इस नीति को लागू करने के लिए विभागाध्यक्ष या उसके अधिकृत अधिकारी जिम्मेदार हैं।

121. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी. एक्ट, 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–20: अभिगम नियंत्रण

122. प्रयोजन

इस नीति का प्रयोजन यह सुनिश्चित करना है कि यूकेएसडीसी संगठन की सूचना परिसंपत्तियों तक सुरक्षित तरीके से पहुंच को प्रतिबंधित करने के लिए प्रक्रियाओं को परिभाषित, विकसित और उपायों को लागू किया गया है।

123. नीति कथन और उद्देश्य

यह नीति यूकेएसडीसी के उपयोगकर्ताओं, ऑपरेटिंग सिस्टम, एप्लिकेशन, डाटाबेस, सुरक्षा और नेटवर्क उपकरणों के लिए अभिगम नियंत्रण नीति को परिभाषित करेगी। इसमें ऐसे कर्मचारी भी शामिल हैं जिनके पास यूकेएसडीसी की सुविधा में रहने वाले किसी भी सिस्टम पर खाता या किसी भी प्रकार की पहुंच है।

124. नियंत्रण

उपयोगकर्ता लॉगिन

1. प्रत्येक उपयोगकर्ता के पास एक विशिष्ट उपयोगकर्ता–आईडी होना चाहिए, जिसे उपयोगकर्ताओं के बीच साझा नहीं किया जाना चाहिए।
   1.1 समूह के भीतर साझा करने के लिए समान लॉगिन क्रेडेंशियल वाले उपयोगकर्ताओं के पूरे समूह के लिए एक आईडी नहीं बनाई जानी चाहिए।
2. आईटी टीम को प्रत्येक पदनाम से जुड़े न्यूनतम अभिगम अधिकारों के एक सेट की पहचान करनी चाहिए और नए उपयोगकर्ता बनाए जाने पर उन्हें सौंपना चाहिए।
3. किसी भी अतिरिक्त विशेषाधिकार को उचित प्राधिकार के बाद ही सौंपा जाएगा।
4. आईटी टीम को सभी निर्दिष्ट उपयोगकर्ता–आईडी और आवंटित विशेषाधिकारों का रिकॉर्ड बनाए रखना चाहिए।
5. उपयोगकर्ताओं को सौंपे गए अभिगम अधिकारों की हर छह माह में समीक्षा की जानी चाहिए।

6. उपयोगकर्ता पहचान प्रक्रिया

निम्नलिखित प्रकार की प्रमाणीकरण योजनाओं का उपयोग करके उपयोगकर्ता की पहचान की जा सकती है:–

6.1 एकल–कारक प्रमाणीकरण:

6.1.1 यह प्रमाणीकरण का सबसे बुनियादी रूप है। एकल–कारक प्रमाणीकरण के लिए केवल एक स्तर, एक पहचान इकाई का उत्पादन करने की आवश्यकता होती है।

6.1.2 आम तौर पर पहचान को "उपयोगकर्ता क्या जानता है" के रूप में वर्गीकृत किया जाता है। आमतौर पर एक्सेस पासवर्ड इसी श्रेणी में आता है।

6.2 दो–कारक प्रमाणीकरण:

6.2.1 यह एकल–कारक प्रमाणीकरण के लिए एक और स्तर की पहचान की मांग करता है। सफल प्रमाणीकरण दोनों शर्तों को पूरा करने की मांग करेगा, केवल एक को संतुष्ट करने से प्रमाणीकरण प्रयास विफल हो जाएगा।

6.2.2 दो–कारक प्रमाणीकरण को "उपयोगकर्ता क्या जानता है और उपयोगकर्ता के पास क्या है" के रूप में वर्गीकृत किया गया है। आमतौर पर एक्सेस पासवर्ड के साथ स्मार्ट (प्लास्टिक) कार्ड का उपयोग किया जाता है।

6.3 तीन–कारक प्रमाणीकरण:

6.3.1 तीन–कारक प्रमाणीकरण पहचान की बायोमेट्रिक तकनीकों का उपयोग करने वाली सबसे मजबूत प्रमाणीकरण योजना है।

6.3.2 तीन–कारक प्रमाणीकरण को "उपयोगकर्ता क्या जानता है, उपयोगकर्ता के पास क्या है और उपयोगकर्ता क्या है" के रूप में वर्गीकृत किया गया है। एक्सेस कार्ड के लिए एक्सेस कार्ड और पासवर्ड के साथ फिंगरप्रिंट स्कैनिंग डिवाइस का उपयोग इस श्रेणी में आता है।

125. अभिगम नियंत्रण

1. सभी इलेक्ट्रॉनिक सूचना जो संवेदनशील, महत्वपूर्ण या मूल्यवान है, उसके पास सिस्टम अभिगम नियंत्रण होना चाहिए।
2. महत्वपूर्ण सूचना की सुरक्षा सुनिश्चित करने के लिए सिस्टम अभिगम की सभी परतों को पर्याप्त रूप से संरक्षित किया जाना चाहिए। विभिन्न परतें जहां अभिगम नियंत्रण लागू किया जा सकता है:

2.1 नेटवर्क लेयर

2.1.1 नेटवर्क स्तर पर, एक्सेस फिल्टरिंग तंत्र जैसे फायरवॉल और राउटर पर अभिगम नियंत्रण लिस्ट के माध्यम से अभिगम नियंत्रण प्राप्त किया जा सकता है। अभिगम नियंत्रण में लगे इन उपकरणों में क्षमता होनी चाहिए और कौन, कहां और कब सिद्धांत के आधार पर केवल अधिकृत उपयोगकर्ताओं को अनुमति देने के लिए कॉन्फिगर किया जाना चाहिए।

2.1.2 कौन – उपयोगकर्ता को या तो उपयोगकर्ता नाम और पासवर्ड के लिए संकेत देकर या उपयोगकर्ता के नेटवर्क पते के आधार पर प्रमाणित किया जाना चाहिए। उच्च सुरक्षा क्षेत्रों के लिए लॉगिन पासवर्ड और स्रोत नेटवर्क एड्रेस सीमा दोनों का संयोजन होना चाहिए।

2.1.3 कहाँ – उपयोक्ता केवल उन प्रणालियों तक पहुँचने में सक्षम होना चाहिए जहाँ उपयोक्ता अभिगम वांछित है और अभिगम केवल सेवाओं, तंत्रों पर पोर्ट्स को अधिकृत करने तक सीमित होना चाहिए।

2.1.4 कब – उपयोगकर्ता केवल व्यावसायिक कार्यावधि के दौरान सिस्टम तक पहुंचने में सक्षम होना चाहिए, इनके अपवादों के लिए गतिविधि के उद्देश्य का उल्लेख करते हुए उचित प्राधिकरण की आवश्यकता होगी।

2.2 **ऑपरेटिंग सिस्टम लेयर**

2.2.1 एक ऑपरेटिंग सिस्टम में, उपयोगकर्ता के विशेषाधिकारों को कम से कम विशेषाधिकार सिद्धांत के आधार पर निर्दिष्ट किया जाना चाहिए और

2.2.2 सभी उपयोगकर्ता विशेषाधिकार समय–आधारित, विक्रेता और अनुबंधों, परीक्षण खातों के लिए विशेष होने चाहिए।

2.2.3 समय अवधि की समाप्ति के बाद उपयोगकर्ता की आवश्यकता और नीति दिशानिर्देशों के अनुसार उपयोगकर्ता विशेषाधिकारों को पुनः निर्दिष्ट किया जाना चाहिए।

2.2.4 30 दिनों की निष्क्रियता के बाद, खाता अक्षम कर दिया जाएगा और उचित अनुमोदन के बाद खोला जा सकता है। यदि 90 दिनों के भीतर खाता सक्रियण के लिए कोई अनुरोध प्राप्त नहीं होता है, तो खाते को निष्क्रिय ओयू में स्थानांतरित कर दिया जाएगा। यदि आईडी डोमेन में नहीं है तो इन आईडी को हटा दिया जाएगा।

2.2.5 उपयोगकर्ता की भूमिका के अनुसार फाइल और फोल्डर स्तर की अनुमतियों को परिभाषित किया जाना चाहिए।

2.3 एप्लिकेशन परत

2.3.1 एप्लिकेशन स्तर पर, प्रत्येक एप्लिकेशन को उपयोगकर्ताओं को मान्य करने के लिए सशक्त प्रमाणीकरण योजनाओं का समर्थन करना चाहिए।

2.3.2 एप्लिकेशन द्वारा प्रदान किए गए उपयोगकर्ता इंटरफेस को ऑपरेटिंग सिस्टम कमांड को निष्पादित करने की अनुमति नहीं देनी चाहिए।

2.4 डाटाबेस

2.4.1 डाटाबेस में संग्रहीत उपयोगकर्ता क्रेडेंशियल को एन्क्रिप्ट किया जाना चाहिए।

2.4.2 डाटाबेस को SQL–इंजेक्शन जैसे हमलों के लिए प्रवण नहीं होना चाहिए; SQL इंजेक्शन डाटाबेस में डाटा पर हमला करने का एक तरीका है।

2.5 जैसे ही इसकी आवश्यकता समाप्त हो, सभी यूजर–आईडी खातों को यथाशीघ्र हटा दिया जाना चाहिए। इसमें निम्नलिखित शामिल हो सकते हैं:

2.5.1 उपयोगकर्ता संगठन छोड़ रहा है।

2.5.2 सलाहकार असाइनमेंट पूरा कर रहा है।

2.5.3 परीक्षण और अस्थायी उपयोगकर्ता खातों को हटाया जाना चाहिए।

2.5.4 एप्लीकेशन को चरणबद्ध तरीके से हटाया जा रहा है।

3. यदि मौजूदा यूजर–आईडी/पासवर्ड को समस्या निवारण के लिए अन्य कर्मियों के साथ साझा किया जाना है, तो इन्हें संबंधित उपयोगकर्ताओं द्वारा उपयोग के तुरंत बाद बदल दिया जाना चाहिए।

4. यदि कोई कंप्यूटर या सुरक्षा उपकरण ठीक से काम नहीं कर रहा है, तो उसे डिफॉल्ट रूप से अंतिम–उपयोगकर्ताओं को विशेषाधिकारों तक पहुंच प्रदान नहीं करनी चाहिए।

4.1 यदि एक्सेस कंट्रोलिंग और फिल्टरिंग डिवाइस, क्रिटिकल सर्वर इत्यादि जैसे महत्वपूर्ण सिस्टम के कुछ घटक, हार्डवेयर या सॉफ्टवेयर खराब हैं, उदाहरण के लिए सिस्टम आवश्यक सेवा चलाने में

सक्षम नहीं है तो इसे उपयोगकर्ता को किसी भी एक्सेस की अनुमति नहीं देनी चाहिए जब तक कि उसे सामान्य रूप में वापस नहीं किया जाता है।

4.2 डिवाइस जो फायरवॉल की तरह विफल हो सकते हैं, उन्हें किसी भी संचार को अनियंत्रित तरीके से पारित करने की अनुमति नहीं देनी चाहिए, इसे बहाल होने तक सभी अभिगम प्रयासों को अवरुद्ध करना चाहिए। ये डिवाइस फेल ओपन होने के बजाय फेल–सेफ होने चाहिए।

5. सभी अभिगम अधिकार संयोजन समय पर सीमित होने चाहिए

5.1 महत्वपूर्ण प्रकार के उपकरणों, महत्वपूर्ण सर्वरों, नेटवर्किंग उपकरणों, सुरक्षा उपकरणों आदि पर सभी पहुंच अधिकार सीमित समय अवधि के लिए वैध होने चाहिए।

5.2 उच्च–जोखिम वाले अनुप्रयोगों और नेटवर्क उपकरणों को निष्क्रियता की एक निर्धारित अवधि (1 मिनट) के बाद सत्र टाइम–आउट करना चाहिए।

6. सभी प्रणालियों की घड़ियों को समकालिक किया जाना चाहिए

6.1 सभी उपकरणों, सर्वरों, नेटवर्किंग उपकरणों, सुरक्षा उपकरणों की घड़ियों को सिंक्रोनाइज़ किया जाना चाहिए, इस प्रकार के उपकरणों द्वारा दिखाया गया समय हर समय एक जैसा होना चाहिए। सिस्टम द्वारा उत्पन्न सभी लॉग स्थानीय सिस्टम समय के साथ टाइम–स्टैम्प्ड हैं इसलिए त्रुटि मुक्त लॉग विश्लेषण की सुविधा के लिए इन प्रणालियों द्वारा बनाए गए स्थानीय समय में कोई विसंगति नहीं होनी चाहिए।

7. लॉगिन बैनर महत्वपूर्ण सर्वरों, एप्लिकेशन, नेटवर्किंग उपकरणों और सुरक्षा उपकरणों पर कॉन्फ़िगर किए जाने चाहिए जो केवल अधिकृत उपयोगकर्ताओं तक पहुंच का सुझाव देते हैं।

8. सिस्टम उपयोगिताओं तक पहुंच केवल व्यवस्थापकों तक ही सीमित होनी चाहिए।

9. सर्वर या डाटा सेंटर रूम तक पहुंच केवल अधिकृत उपयोगकर्ताओं तक ही सीमित होनी चाहिए।

10. महत्वपूर्ण सर्वरों के लिए स्थानीय या दूरस्थ पहुँच; नेटवर्क और सुरक्षा उपकरणों को सुरक्षित किया जाना चाहिए। पासवर्ड एन्क्रिप्टेड मोड में भेजा जाना चाहिए।

10.1 उदाहरण के लिए, टेलनेट का उपयोग फायरवॉल या नेटवर्क राउटर तक पहुँचने के लिए नहीं किया जाना चाहिए, सुरक्षित लॉग–ऑन के लिए SSH का उपयोग करें।

126. इंटरनेट का उपयोग

1. यूकेएसडीसी के डोमेन/नेटवर्क से जुड़े सभी उपयोगकर्ताओं को इंटरनेट का उपयोग केवल एक केन्द्रीय गेटवे से करना चाहिए।

1.1 जो उपयोगकर्ता यूकेएसडीसी के डोमेन/नेटवर्क का हिस्सा नहीं हैं, उन्हें इस गेटवे से इंटरनेट एक्सेस की अनुमति नहीं दी जानी चाहिए।

1.2 यदि किसी विक्रेता या उपयोगकर्ता को एक्सेस की आवश्यकता होती है, तो प्रबंधन से अनुमोदन लिया जाना चाहिए और यह सुनिश्चित करने के लिए सिस्टम पर जांच की जानी चाहिए कि सिस्टम सुरक्षित है और नवीनतम सुरक्षा पैच और एंटी–वायरस अपडेट के साथ अद्यतन है।

2. उपयोगकर्ताओं को उनके संबंधित विभागों से अनुमोदन के बाद ही इंटरनेट की सुविधा प्रदान की जानी चाहिए।

3. यूजर–आईडी/आई.पी.–आधारित प्रमाणीकरण का उपयोग करके इंटरनेट एक्सेस को नियंत्रित किया जाना चाहिए।
4. इंटरनेट कनेक्शन को फायरवॉल के माध्यम से सुरक्षित किया जाना चाहिए।
5. फायरवॉल को इंटरनेट प्रॉक्सी में किसी भी इनबाउंड एक्सेस को रोकना चाहिए।
6. सभी इंटरनेट ट्रैफिक को स्कैन करने के लिए इंटरनेट गेटवे पर गेटवे एंटी–वायरस सॉफ़्टवेयर स्थापित किया जाना चाहिए। एंटी–वायरस को निम्न के लिए कॉन्फ़िगर किया जाना चाहिए:
   6.1 जब भी कोई उपयोगकर्ता किसी फाइल को डाउनलोड/अपलोड करता है, तो उसे वायरस के लिए स्कैन किया जाना चाहिए।
   6.2 यदि कोई वायरस पाया जाता है, तो डाउनलोड/अपलोड समाप्त हो जाना चाहिए और उपयोगकर्ताओं को स्थिति के बारे में सूचित किया जाता है।
7. एक्सेस कंट्रोल लिस्ट को बाउंड्री राउटर पर लागू किया जाना चाहिए ताकि कमजोर पोर्ट्स तक पहुंच को अवरुद्ध किया जा सके।
8. जिन पोर्ट्स को वायरस/वर्म्स या किसी अन्य हमले के प्रति संवेदनशील माना जाता है, उन्हें अवरुद्ध कर दिया जाना चाहिए।

127. आंतरिक नेटवर्क का उपयोग

1. यदि आंतरिक नेटवर्क पर पहुंच की आवश्यकता है, तो उपयोगकर्ता मशीन को यूकेएसडीसी के सुरक्षा मानकों को पूरा करना चाहिए। यूकेएसडीसी के डेस्कटॉप या किसी तीसरे पक्ष के लैपटॉप के माध्यम से आंतरिक नेटवर्क तक पहुंच प्रदान की जा सकती है। यदि यह यूकेएसडीसी द्वारा प्रदान किया गया डेस्कटॉप है, तो इसे डेस्कटॉप के लिए सुदृढ़ अभिलेख के अनुसार बनाया जाना चाहिए। यह सुनिश्चित किया जाना चाहिए कि केवल कार्य के लिए आवश्यक सॉफ़्टवेयर स्थापित किया गया है। यदि तीसरे पक्ष के कर्मियों के लैपटॉप के माध्यम से पहुंच प्रदान की जाती है, तो यह सुनिश्चित किया जाना चाहिए कि एंटी–वायरस सुरक्षा सक्षम है, और सभी आवश्यक सुरक्षा पैच स्थापित किए गए हैं।

128. सर्वर और यूजर सेगमेंट को पृथक करना

1. महत्वपूर्ण सर्वरों को फायरवॉल द्वारा उपयोगकर्ता खंडों (यूजर सेगमेंट) से अलग किया जाना चाहिए।
2. फायरवॉल को संबंधित सर्वर पर आवश्यक पोर्ट तक उपयोगकर्ता की पहुँच को प्रतिबंधित करना चाहिए।

129. बाह्य पहुंच

1. यूकेएसडीसी के सुरक्षा प्रबंधन से बाहर के बाह्य नेटवर्क से जुड़ने से पहले सभी उपयोगकर्ताओं को सी.आई.एस.ओ. से पूर्व अनुमोदन प्राप्त करना चाहिए।
   1.1 सी.आई.एस.ओ. को कनेक्शन से जुड़े सुरक्षा जोखिमों का आकलन करना चाहिए और जोखिम को कम करने के लिए आवश्यक कदमों की अनुशंसा करनी चाहिए। संयोजन को सक्षम करने से पहले अनुशंसित नियंत्रणों को लागू किया जाना चाहिए।

2. यूकेएसडीसी नेटवर्क तक रिमोट एक्सेस को नियंत्रित करना चाहिए और इसमें उचित प्रमाणीकरण तंत्र होना चाहिए, उपयोगकर्ताओं के लिए वी.पी.एन.या एचटीटीपीएस या एन्क्रिप्शन लॉजिक/स्क्रिप्ट–आधारित पहुंच प्रदान करें।

130. **लॉगिंग**

1. प्रमाणीकरण विफलताओं या उपकरणों पर किसी भी प्रकार के हमलों को रिकॉर्ड करने के लिए महत्वपूर्ण उपकरण, महत्वपूर्ण सर्वर, नेटवर्किंग उपकरणों और सुरक्षा उपकरणों पर लॉगिंग सक्षम होनी चाहिए।
2. घुसपैठ का पता लगाने वाली प्रणाली (आईडीएस) लागू करें जो ज्ञात हमलों, असामान्य व्यवहार, अनधिकृत पहुंच के प्रयासों और नीति के उल्लंघन जैसी गतिविधि के लिए वास्तविक समय में नेटवर्क की निगरानी करता है।

131. **स्पष्ट डेस्क और स्पष्ट स्क्रीन नीति**

1. कागजात और हटाने योग्य स्टोरेज मीडिया के लिए एक स्पष्ट डेस्क नीति और सूचना प्रसंस्करण सुविधाओं के लिए एक स्पष्ट स्क्रीन नीति अपनाई जानी चाहिए। कागज या इलेक्ट्रॉनिक स्टोरेज मीडिया जैसी संवेदनशील या महत्वपूर्ण व्यावसायिक सूचना को एक सुरक्षित या अग्निरोधक कैबिनेट में बंद कर दिया जाना चाहिए।
2. संवेदनशील अभिलेखों या वर्गीकृत सूचना को प्रिंटर से तुरंत हटा दिया जाना चाहिए और इसे अप्राप्य नहीं छोड़ा जाना चाहिए।
3. प्रिंट आउट को अप्राप्य नहीं छोड़ा जाना चाहिए।
4. इनकमिंग और आउटगोइंग मेल पॉइंट्स और अनअटेंडेड फैक्सीमाइल मशीनों को संरक्षित किया जाना चाहिए
5. फोटोकॉपियर, स्कैनर और डिजिटल कैमरों जैसी प्रतिकृति तकनीक को नियंत्रित और मॉनिटर किया जाना चाहिए।
6. कंप्यूटर और टर्मिनलों को लॉग ऑफ छोड़ दिया जाना चाहिए।
7. स्क्रीन सेवर सभी सर्वर, डेस्कटॉप और लैपटॉप के लिए सक्षम होना चाहिए। (5 मिनट हेतु)

132. **प्रयोज्यता**

यह नीति यूकेएसडीसी के सभी हितधारकों के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की गई है।

133. **प्रवर्तन एवं व्याख्या**

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–21: एप्लिकेशन सुरक्षा

134. प्रयोजन

इस नीति का प्रयोजन यह सुनिश्चित करना है कि यूकेएसडीसी संगठन यह सुनिश्चित करने के लिए पर्याप्त नियंत्रणों को परिभाषित, विकसित और कार्यान्वित करता है कि सभी एप्लिकेशन सुरक्षा आवश्यकताओं को पूरा करते हैं।

135. नीति कथन और उद्देश्य

इस नीति का उद्देश्य यह सुनिश्चित करना है कि यूकेएसडीसी में तैनात एप्लिकेशन्स में डाटा के सुरक्षित इनपुट, प्रसंस्करण, भंडारण और आउटपुट के लिए नियंत्रण होना चाहिए। एप्लिकेशन्स को परिनियोजन से पहले सुरक्षा और प्रदर्शन के लिए परीक्षण किया जाना चाहिए और उच्च उपलब्धता के लिए प्रबंधित किया जाना चाहिए। एप्लिकेशन्स तक पहुंच अधिकृत व्यक्तियों और न्यूनतम विशेषाधिकार के सिद्धांत पर प्रदान किए गए अधिकारों तक सीमित होनी चाहिए। यह नीति यूकेएसडीसी में सभी एप्लिकेशन्स पर लागू होती है।

136. नियंत्रण

एप्लिकेशन धारक

1. यूकेएसडीसी के भीतर परिनियोजित सभी एप्लिकेशन के लिए एक निर्दिष्ट धारक होना चाहिए। एप्लिकेशन डिजाइन, विकास, परिनियोजन और समर्थन से संबंधित सभी गतिविधियों की जिम्मेदारी एप्लिकेशन धारक की होनी चाहिए।
   1.1 एप्लिकेशन धारक को विभाग प्रमुख द्वारा नामित किया जाना चाहिए।

137. एप्लिकेशन अभिगम

1. एप्लिकेशन में अभिगम की अनुमति देने से पहले सभी उपयोगकर्ताओं को प्रमाणित करने की सुविधा होनी चाहिए।
2. एप्लिकेशन को यह सुनिश्चित करना चाहिए कि सभी संव्यवहार में एक अलग अनुरोधकर्ता और अनुमोदक है। अपने ग्रेड, शीर्षक, या कार्य के बावजूद कोई भी व्यक्ति संवेदनशील, मूल्यवान, या महत्वपूर्ण सूचना से संबंधित संव्यवहार को प्रारम्भ करने से लेकर अंतिम प्राधिकरण तक पूरा नहीं करेगा।
   2.1 इसका मतलब यह है कि संव्यवहार को पूरा होने से पहले कम से कम एक व्यक्ति के हस्तक्षेप की आवश्यकता होगी। इसी तरह, किसी एक व्यक्ति को अपने स्वयं के कार्य को अनुमोदित करने के लिए उत्तरदायी नहीं होना चाहिए।
3. एप्लिकेशन के भीतर एकाधिक विशेषाधिकार स्तरों के लिए प्रावधान होना चाहिए।
   3.1 एप्लिकेशन में न्यूनतम विशेषाधिकार के सिद्धांत के आधार पर पहुंच अधिकार आवंटित करने का प्रावधान होना चाहिए।

3.2 एप्लिकेशन से जुड़े विशेषाधिकार स्तर और कर्मचारियों की श्रेणियां जिनके लिए उन्हें आवंटित किया जाना चाहिए, उन्हें एप्लिकेशन के मालिक द्वारा पहचाना और प्रलेखित किया जाना चाहिए।

3.3 एप्लिकेशन के मालिक को यह सुनिश्चित करना चाहिए कि एप्लिकेशन के भीतर विशेषाधिकार स्तर स्टाफ सदस्य की विवेकाधीन शक्तियों के अनुरूप हैं।

3.4 एप्लिकेशन को जानने की आवश्यकता और करने की आवश्यकता के आधार पर मेनू विकल्पों को प्रतिबंधित करना चाहिए।

4. लॉग इन करने के बाद, सभी अंतिम–उपयोगकर्ताओं को मेनू में रखा जाना चाहिए, जो उन विकल्पों को दिखाते हैं जिन्हें चुनने के लिए उन्हें अधिकृत किया गया है।

4.1 अंतिम–उपयोगकर्ताओं को ऑपरेटिंग सिस्टम–स्तरीय कमांड को लागू करने की अनुमति नही दी जानी चाहिए।

5. सभी एप्लिकेशन यूजर्स को संबंधित यूजर मैनेजर/टीम लीडर/विभाग से अनुमोदन के बाद ही बनाया जाना चाहिए।

5.1 संबंधित यूजर मैनेजर/टीम लीडर/विभाग को सिस्टम एडमिनिस्ट्रेटर/एप्लिकेशन डेवलपर को एप्लिकेशन पर यूजर अकाउंट बनाने के लिए प्राधिकरण के लिए एक अनुरोध भेजना चाहिए।

6. "न्यूनतम पहुंच", "कार्यों का पृथक्करण", और "जानने की आवश्यकता" के सिद्धांतों को यूकेएसडीसी के अनुप्रयोगों तक पहुंचने के लिए उपयोगकर्ता प्राधिकरणों के निर्धारण का मार्गदर्शन करना चाहिए।

7. एक सफल लॉग–ऑन के पूरा होने पर एप्लिकेशन को निम्नलिखित जानकारी प्रदर्शित करनी चाहिए:

7.1 पिछले सफल लॉगऑन की तिथि और समय।

7.2 अंतिम सफल लॉगिन के बाद से किसी भी असफल लॉगिन प्रयास का विवरण।

8. उपयोगकर्ता आईडी में उपयोगकर्ता के विशेषाधिकार स्तर का कोई संकेत नहीं देना चाहिए।

9. एक उपयोगकर्ता को अपने विशेषाधिकार स्तर के समान उपयोगकर्ता आईडी नहीं चुननी चाहिए, उदाहरण के लिए एक प्रबंधक को अपने उपयोगकर्ता आईडी के रूप में प्रबंधक का उपयोग नहीं करना चाहिए।

10. यूकेएसडीसी सिस्टम पर विशेष सिस्टम या एप्लिकेशन विशेषाधिकार (मास्टर आईडी/आपातकालीन पासवर्ड) सिस्टम प्रबंधन और/या सुरक्षा के लिए सीधे तौर पर जिम्मेदार लोगों तक ही सीमित होना चाहिए। प्रत्येक उपयोग के बाद पासवर्ड बदलना होगा।

11. प्रमाणीकरण उद्देश्यों के लिए एप्लिकेशन को लॉगिन क्रेडेंशियल को दूसरे पृष्ठ पर पुनर्निर्देशित करना चाहिए। यह सुनिश्चित करने के लिए है कि कोई दुर्भावनापूर्ण उपयोगकर्ता एप्लिकेशन में अनधिकृत प्रविष्टि प्राप्त करने के लिए 'बैक–बैक–रिफ्रेश' विकल्प का उपयोग नहीं कर सकता है।

138. डाटा सुरक्षा

1. एप्लिकेशन उपयोगकर्ता लॉगिन क्रेडेंशियल सहित संवेदनशील डाटा को एन्क्रिप्टेड प्रारूप में संग्रहीत किया जाना चाहिए।

1.1 उपयोगकर्ता लॉगिन पासवर्ड को सुरक्षित तरीके से संग्रहित किया जाना चाहिए। उपयोगकर्ता पासवर्ड को इस तरह से संग्रहित किया जाना चाहिए कि इसे सिस्टम प्रशासक/एप्लिकेशन डेवलपर द्वारा भी

पुनर्प्राप्त नहीं किया जा सकता है। इसे लागू करने के लिए एक तरह से हैशिंग तंत्र का उपयोग किया जा सकता है।

2. एप्लिकेशन में डाटा की अखंडता की जांच करने की सुविधा होनी चाहिए।
3. एप्लिकेशन धारक को एप्लिकेशन द्वारा प्रबंधित सभी डाटा के लिए प्रतिधारण अवधि को परिभाषित करना चाहिए।
   - 3.1 यह प्रासंगिक वैधानिक और नियामक आवश्यकताओं पर विचार करने के बाद किया जाना चाहिए।
   - 3.2 बैकअप मीडिया रोटेशन चक्र का निर्धारण करने के लिए और फ्री डिस्क स्थान बनाने के लिए पुराने डाटा को मिटाने का निर्णय लेने के लिए एक प्रतिधारण अवधि की आवश्यकता होती है।
4. एप्लिकेशन सर्वर को ओएस और एप्लिकेशन के लिए सुरक्षा पैच के साथ सुदृढ़ और अद्यतन किया जाना चाहिए।

139. इनपुट नियंत्रण

1. यह सुनिश्चित करने के लिए कि यह उचित और अपेक्षित दोनों है, एप्लिकेशन द्वारा सभी उपयोगकर्ता इनपुट की जाँच की जानी चाहिए।
   - 1.1 सॉफ्टवेयर में यह सुनिश्चित करने के लिए पर्याप्त नियंत्रण होना चाहिए कि डाटा सटीक रूप से इनपुट किया गया है जैसे रेंज चेक, वैधता जांच इत्यादि।
   - 1.2 प्रत्येक संव्यवहार को इस तरह से रिकॉर्ड किया जाना चाहिए कि यह स्थापित किया जा सके कि यह सिस्टम में इनपुट किया गया है।
   - 1.3 एप्लिकेशन में यह सुनिश्चित करने के लिए अतिरिक्त नियंत्रण होना चाहिए कि सभी रिकॉर्ड किए गए संव्यवहार सिस्टम में इनपुट हैं और केवल एक बार स्वीकार किए जाते हैं।
   - 1.4 अस्वीकृत संव्यवहार की सूचना दी जानी चाहिए।
2. बैच कार्य को दिशानिर्देशों के एक सेट का पालन करना चाहिए:
   - 2.1 यह सुनिश्चित करने के लिए नियंत्रण होना चाहिए कि सभी प्रविष्टियां बिना किसी चूक के अपलोड कर दी गई हैं।
   - 2.2 अपलोड किए गए डाटा की अखंडता को सत्यापित करने के लिए हैश योग का उपयोग किया जाना चाहिए।
   - 2.3 यदि वे अचानक समाप्त हो जाते हैं तो बैच कार्य के लिए पुनरारंभ सुविधा होनी चाहिए।
   - 2.4 यह सुनिश्चित करने के लिए नियंत्रण होना चाहिए कि बैच कार्य के पुनरारंभ के दौरान कोई त्रुटि न हो।
   - 2.5 बैच कार्य निष्पादित करने वाले व्यक्ति का उपयोगकर्ता–आईडी संव्यवहार में अंतर्निहित किया जाना चाहिए।
   - 2.6 बैच प्रक्रियाओं के लिए एक इवेंट लॉग होना चाहिए।
   - 2.7 यदि बैच कार्य द्वारा बनाई गई कोई अस्थायी फाइलें हैं, तो उन्हें कार्य समाप्त होने से पहले हटा दिया जाना चाहिए।

2.8 यदि प्रक्रिया केवल एक बार की जानी है, तो एप्लिकेशन को यह सुनिश्चित करना चाहिए कि प्रक्रिया को एक से अधिक बार निष्पादित नहीं किया गया है।

2.9 यदि एक बैच प्रक्रिया के भीतर कई कार्य हैं जिन्हें क्रमिक रूप से निष्पादित करने की आवश्यकता है, तो यह सुनिश्चित करने के लिए नियंत्रण होना चाहिए कि एक नया कार्य पिछले एक के सफलतापूर्वक पूरा होने के बाद ही लिया जाए। यदि कोई एक कार्य विफल हो जाता है, तो प्रक्रिया को शेष कार्यों को जारी रखे बिना बाहर निकल जाना चाहिए।

2.10 यदि भिन्नता को दूर करने के लिए सुधार किए जाने हैं, तो परिवर्तन से पहले इन्हें उपयुक्त प्राधिकारी द्वारा अनुमोदित किया जाना चाहिए।

2.11 यदि दो उपयोगकर्ता एक ही समय में एक ही रिकॉर्ड तक पहुंच रहे हैं, तो एप्लिकेशन को डाटाबेस स्थिरता सुनिश्चित करनी चाहिए। असंगति और खोए हुए अद्यतनों को रोकने के लिए, डाटाबेस अनुप्रयोग में लॉकिंग को लागू करने की आवश्यकता है।

140. प्रसंस्करण नियंत्रण

1. एप्लिकेशन को यह सुनिश्चित करना चाहिए कि प्रक्रियाओं को क्रम से शुरू नहीं किया जा सकता है। एप्लिकेशन को यह सुनिश्चित करना चाहिए कि किसी विशेष प्रक्रिया से जुड़े सभी कार्य पूरे हो गए हैं और उनमें हेरफेर या बायपास नहीं किया जा सकता है।
2. एप्लिकेशन में यह सुनिश्चित करने के लिए अंतर्निहित जांच होनी चाहिए कि यदि किसी विशेष प्रक्रिया को क्रियान्वित करने के लिए कोई पूर्व–आवश्यकताएं हैं, तो इसे शुरू करने से पहले पूरी की जाती हैं।

141. प्रदर्शन का परीक्षण

एप्लिकेशन धारक को यह सुनिश्चित करना चाहिए कि अभिनियोजित करने से पहले पीक लोड स्थितियों के लिए एप्लिकेशन का परीक्षण किया जाता है। सभी बहु–उपयोगकर्ता एप्लिकेशन के लिए, लोड परीक्षण को ऐसे वातावरण में करने की आवश्यकता होती है जो वास्तविक जीवन स्थितियों का अनुकरण करते हैं।

142. अकाउंट नीति

1. एप्लिकेशन को कम से कम 8 वर्णों की पासवर्ड लंबाई लागू करनी चाहिए। महत्वपूर्ण एप्लिकेशन के लिए जो केवल आंतरिक उपयोगकर्ताओं द्वारा उपयोग किए जाते हैं, न्यूनतम पासवर्ड लंबाई 8 वर्णों का उपयोग किया जाना चाहिए। पासवर्ड नीति का संदर्भ लें।
2. पासवर्ड की समाप्ति 90 दिनों की अवधि पर निर्धारित की जानी चाहिए। उन महत्वपूर्ण एप्लिकेशन हेतु जिन्हें केवल आंतरिक उपयोगकर्ताओं द्वारा एक्सेस किया जाता है, न्यूनतम पासवर्ड समाप्ति को कम समयावधि जैसे 45 दिनों पर निर्धारित किया जाना चाहिए।
3. एप्लिकेशन में एक खाता (अकाउंट) लॉकआउट सुविधा कॉन्फिगर की गई होनी चाहिए।
   3.1 5 असफल लॉगिन प्रयासों के बाद एप्लिकेशन को उपयोगकर्ता खाते को लॉक कर देना चाहिए।
   3.2 लॉक किए गए खातों को सिस्टम व्यवस्थापक द्वारा मैन्युअल रूप से जारी किया जा सकता है या 24 घंटों के बाद एप्लिकेशन द्वारा स्वचालित रूप से अनलॉक किया जा सकता है।

4. पासवर्ड हिस्ट्री को मेंटेन करना चाहिए। अंतिम 5 पासवर्ड प्रयोग करने योग्य नहीं होने चाहिए।
5. उपयोगकर्ता को विशेषाधिकार प्राप्त और सामान्य (गैर–विशेषाधिकार प्राप्त) गतिविधियों को करने के लिए अलग उपयोगकर्ता आईडी की अनुमति दी जाएगी, उदाहरण के लिए, एक प्रशासन उद्देश्यों के लिए और दूसरा एप्लिकेशन का उपयोग करने के लिए।
6. एप्लिकेशन को नए उपयोगकर्ता को पहले लॉगिन पर पासवर्ड बदलने के लिए बाध्य करना चाहिए।
7. उपयोगकर्ता खाते जो एप्लिकेशन की डिफॉल्ट स्थापना का हिस्सा हैं, लेकिन सामान्य संचालन के लिए आवश्यक नहीं हैं, उन्हें अक्षम किया जाना चाहिए।
8. एप्लिकेशन को 30 मिनट तक बिना किसी गतिविधि (सत्र का समय समाप्त) के बाद स्क्रीन लॉक कर देनी चाहिए। उपयोगकर्ता पासवर्ड प्रदान करने के बाद ही स्क्रीन को फिर से सक्रिय किया जाना चाहिए।

143. ऑडिट लॉग्स और अनुश्रवण

1. एप्लिकेशन में सभी संव्यवहार लॉग करने की सुविधा होनी चाहिए। लॉग ऑडिट ट्रेल प्रदान करते हैं और धोखाधड़ी की स्थिति में दुर्भावनापूर्ण उपयोगकर्ताओं पर नजर रखने में महत्वपूर्ण भूमिका निभाते हैं। लॉग की निगरानी और समीक्षा साप्ताहिक या दैनिक आधार पर की जानी चाहिए। एप्लिकेशन की गंभीरता के आधार पर लॉग की समीक्षा की जा सकती है। (मासिक, साप्ताहिक या दैनिक आधार पर समीक्षा करने के लिए)
2. एप्लिकेशन निम्नलिखित सहित सभी सुरक्षा–संबंधित घटनाओं को लॉग करने में सक्षम होना चाहिए
   - 2.1 उपयोगकर्ता खाता प्रबंधन,
   - 2.2 उपयोगकर्ता के विशेषाधिकार में परिवर्तन,
   - 2.3 उपयोगकर्ता लॉगिन/लॉगआउट समय,
   - 2.4 एप्लिकेशन कॉन्फिगरेशन में परिवर्तन,
   - 2.5 प्रमाणीकरण विफलता,
3. लॉगिंग सिस्टम संसाधनों को लेता है और इसलिए व्यापक लॉगिंग एप्लिकेशन को धीमा कर सकती है। एप्लिकेशन धारकों को यह सुनिश्चित करने की आवश्यकता है कि वित्तीय संव्यवहार और सुरक्षा से संबंधित घटनाओं के बारे में आवश्यक जानकारी प्रदान करने के लिए एप्लिकेशन के भीतर उचित लॉगिंग विधियां प्रदान की जाती हैं।

144. त्रुटि प्रबंधन

1. एप्लिकेशन द्वारा उत्पन्न त्रुटि संदेशों को महत्वपूर्ण सूचना का खुलासा नहीं करना चाहिए।
   - 1.1 त्रुटि अंतिम उपयोगकर्ता को इंगित करने वाली सूचना प्रकट नहीं करनी चाहिए कि सही इनपुट क्या हो सकता है।
   - 1.2 त्रुटि संदेश से एप्लिकेशन या डाटाबेस के बारे में कोई सूचना प्रकट नहीं होनी चाहिए।

145. परिवर्तन प्रबंधन

1. सुरक्षा स्तर को बनाए रखने के लिए, एप्लिकेशन में सभी परिवर्तन उचित प्राधिकार के बाद किए जाने चाहिए।
   - 1.1 व्यवसाय/एप्लिकेशन धारकों को परिवर्तन प्रबंधन समिति (सीएमसी) को अनुरोध देना चाहिए।
   - 1.2 एप्लिकेशन में सभी परिवर्तनों को परिवर्तन प्रबंधन प्रक्रिया का पालन करना चाहिए। किसी भी परिवर्तन से पहले सी.एम.सी. की स्वीकृति प्राप्त की जानी चाहिए।
   - 1.3 परिवर्तन प्रबंधन समिति सुरक्षा निहितार्थों और आवश्यकताओं के आधार पर अनुरोध को स्वीकृत, संशोधित या अस्वीकार करेगी।
   - 1.4 परिवर्तन प्रबंधन समिति परिवर्तन को सत्यापित करने के लिए एक सत्यापनकर्ता को अधिकृत करेगी।
   - 1.5 सत्यापनकर्ता को परिवर्तन प्रबंधन समिति को एक रिपोर्ट देनी चाहिए।
2. परिनियोजन से पहले एप्लिकेशन में सभी परिवर्तनों का परीक्षण किया जाना चाहिए।
   - 2.1 मूल योजना से किसी भी विचलन को भी प्रलेखित किया जाना चाहिए।
   - 2.2 परीक्षण डाटा को अनधिकृत पहुंच से पर्याप्त रूप से सुरक्षित रखा जाना चाहिए।
3. संभावित बाधाओं से बचने के लिए यूकेएसडीसी की सूचना प्रसंस्करण क्षमताओं में व्यापार और सिस्टम आवश्यकताओं और वर्तमान और अनुमानित रुझानों के आधार पर आवेदन में किसी भी बदलाव की सावधानीपूर्वक योजना बनाई जाएगी।
4. नए एप्लिकेशन सिस्टम या अपग्रेड की स्वीकृति के लिए आवश्यकताएं और मानदंड परिभाषित, सहमत, प्रलेखित और परीक्षण किए जाने चाहिए।
5. किसी भी नए एप्लिकेशन के लिए उपयोगकर्ता स्वीकृति परीक्षण और प्रशिक्षण के लिए रिकॉर्ड बनाए रखें।

146. प्रलेखन

1. एप्लिकेशन धारक को यह सुनिश्चित करना चाहिए कि निम्नलिखित गतिविधियों के लिए विस्तृत अभिलेख उपलब्ध हैं:
   - 1.1 एप्लिकेशन संस्थापन,
   - 1.2 कॉन्फ़िगरेशन सेटिंग्स,
   - 1.3 विशेषाधिकार स्तर और संबंधित कर्मचारी श्रेणियां,
   - 1.4 बैकअप और पुनर्प्राप्ति प्रक्रिया,
   - 1.5 बैकअप और पुनर्प्राप्ति आवृत्ति,
   - 1.6 डाटा प्रतिधारण अवधि,
2. सभी अभिलेखों का पर्याप्त बैकअप रखा जाएगा और सभी महत्वपूर्ण अभिलेख और मैनुअल की एक प्रति ऑफ–साइट संग्रहीत की जाएगी।

147. वेब एप्लिकेशन सुरक्षा नियंत्रण

1. वेब इंटरफेस वाले एप्लिकेशन को सॉफ्टवेयर सुरक्षा नियंत्रण के अनुसार लागू और परीक्षण किया जाना चाहिए।

2. वेब एप्लिकेशन को ओ.डब्ल्यू.ए.एस.पी. (द ओपन वेब एप्लीकेशन सिक्योरिटी प्रोजेक्ट) द्वारा निर्धारित दिशानिर्देशों का पालन करना चाहिए, जो एक ओपन सोर्स सुरक्षा समुदाय है, जो वेब सेवाओं की सुरक्षा के अनुसंधान में शामिल है। वेब एप्लिकेशन को निम्नलिखित प्रमुख कमजोरियों से सुरक्षित किया जाना चाहिए

2.1 खंडित सत्र प्रबंधन: यह भेद्यता खाता क्रेडेंशियल और सत्र टोकन की अनुचित सुरक्षा के कारण उत्पन्न होती है। इससे ऐसे हमले हो सकते हैं जो पासवर्ड और सत्र कुकीज़ से समझौता कर सकते हैं और प्रमाणीकरण प्रतिबंधों को बायपास कर सकते हैं।

2.2 क्रॉस–साइट स्क्रिप्टिंग (XSS) खामियां: इस भेद्यता के परिणामस्वरूप वेब एप्लिकेशन का उपयोग अंतिम उपयोगकर्ता के ब्राउज़र पर हमले को पहुंचाने के लिए एक तंत्र के रूप में किया जा सकता है। यह अंतिम उपयोगकर्ता के सत्र टोकन का खुलासा कर सकता है, स्थानीय मशीन पर हमला कर सकता है, या उपयोगकर्ता को झाँसा देना के लिए विषय वस्तु को चकमा दे सकता है।

2.3 बफर ओवरफ्लो: वेब एप्लिकेशन घटक जो इनपुट को ठीक से मान्य नहीं करते हैं, उन्हें क्रैश किया जा सकता है और कुछ मामलों में, एक प्रक्रिया को नियंत्रित करने के लिए उपयोग किया जाता है। इन घटकों में सीजीआई, लाइब्रेरी, ड्राइवर और वेब एप्लिकेशन सर्वर घटक शामिल हो सकते हैं।

2.4 कमांड इंजेक्शन की खामियां: जब वे बाहरी सिस्टम या स्थानीय ऑपरेटिंग सिस्टम तक पहुंचते हैं तो वेब एप्लिकेशन पैरामीटर पास करते हैं। यदि इन मापदंडों में दुर्भावनापूर्ण आदेश अंतर्निहित हैं, तो बाहरी सिस्टम वेब एप्लिकेशन की ओर से उन आदेशों को निष्पादित कर सकता है।

2.5 वेब एप्लिकेशन को ओ.डब्ल्यू.ए.एस.पी. में प्रमुख कमजोरियों के विरूद्ध सुरक्षित किया जाना चाहिए जो सभी यूकेएसडीसी अनुप्रयोगों पर लागू हो सकते हैं। (www-owasp-org) का संदर्भ लें।

148. प्रयोज्यता

यूकेएसडीसी नेटवर्क और इंटरनेट संसाधनों का उपयोग करने वाले सभी हितधारकों की इस नीति का पालन करने की जिम्मेदारी है। सिस्टम एडमिनिस्ट्रेटर और डाटा सेंटर के प्रभारी के पास इस नीति को लागू करने और यह सुनिश्चित करने की जिम्मेदारी है कि इसका पालन किया जा रहा है।

149. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–22: परिवर्तन प्रबंधन

150. प्रयोजन

इस नीति का प्रयोजन यह सुनिश्चित करना है कि यूकेएसडीसी संगठन (यूकेएसडीसी) आईटी अवसंरचना में महत्वपूर्ण परिवर्तनों से जुड़े जोखिमों के प्रबंधन के लिए पर्याप्त नियंत्रणों को परिभाषित, विकसित और कार्यान्वित करता है।

151. नीति कथन और उद्देश्य

इस नीति का उद्देश्य यूकेएसडीसी के आईटी बुनियादी ढांचे में सभी प्रकार के परिवर्तन (महत्वपूर्ण, मानक परिवर्तन आदि) के लिए एक उचित परिवर्तन प्रबंधन प्रक्रिया सुनिश्चित करना है।

152. नियंत्रण

परिवर्तन का वर्गीकरण:

1. आईटी सिस्टम के सभी परिवर्तनों को निम्नलिखित श्रेणियों में से किसी एक में वर्गीकृत करें:

1.1 प्रमुख परिवर्तनों में निम्नलिखित शामिल हैं, लेकिन इन्हीं तक सीमित नहीं हैं:–

1.1.1. नेटवर्क पुनः विन्यास,

1.1.2. ऑपरेटिंग सिस्टम या एप्लीकेशन चेंज/अपग्रेड,

1.1.3. एंटी–वायरस रोल आउट,

1.1.4. लाइव सर्वर, वेब सर्वर, डाटाबेस सर्वर आदि का सख्त होना,

1.1.5. नया भौतिक सर्वर या उपकरण संस्थापन,

1.1.6. सक्रिय निर्देशिका सर्वर और समूह नीति में परिवर्तन,

1.1.7. ई–मेल सेटअप पुनर्विन्यास,

1.1.8. आईटी आपदा पुनर्प्राप्ति,

1.1.9. नवीन नेटवर्क परिवर्धन,

1.1.10. नवीन व्यवसाय एप्लीकेशन,

1.1.11. सर्विस पैक कार्यान्वयन।

टिप्पणी: कोई भी परिवर्तन जो ऑपरेशन फंक्शन को प्रभावित कर सकता है और डाउन टाइम का कारण बन सकता है उसे प्रमुख परिवर्तन के रूप में वर्गीकृत किया जाता है।

1.2 मामूली परिवर्तनों में निम्नलिखित शामिल हैं, लेकिन इन्हीं तक सीमित नहीं हैं:–

1.2.1. अनुप्रयोगों में मामूली बग फिक्स,

1.2.2. एंटी–वायरस रीकॉन्फिगरेशन या अपग्रेड,

1.2.3. फायरवॉल नियम आधार परिवर्तन,

1.2.4. नया पैच कार्यान्वयन।

1.3 आपातकालीन परिवर्तनः प्रमुख परिवर्तन तत्काल प्रभाव से किए जाने हैं जिनके बिना सिस्टम आगे नहीं बढ़ सकता या कार्य नहीं कर सकता है।

1.3.1. विद्युत अवरोध की स्थिति में सिस्टम को बंद किया जाएगा

1.3.2. महत्वपूर्ण कस्टम एप्लिकेशन पैच का परिनियोजन

1.3.3. महत्वपूर्ण सुरक्षा पैच संस्थापन (उदाहरण के लिए जब कोई नया वायरस या वर्म हमला)

153. परिवर्तन प्रबंधन समिति

निदेशक आईटीडीए द्वारा परिवर्तन प्रबंधन समिति का गठन किया जाएगा।

1. महत्वपूर्ण/प्रमुख परिवर्तनों को अनुमोदित करने और उन पर नजर रखने के लिए एक परिवर्तन प्रबंधन समिति (सी.एम.सी.) का गठन करें। संबंधित पी.एम.सी. के पी.एम. द्वारा मामूली बदलावों को मंजूरी दी जा सकती है।
2. सी.एम.सी. में सी.आई.एस.ओ., सिस्टम एडमिनिस्ट्रेटर और प्रोजेक्ट मैनेजर शामिल होने चाहिए।
   2.1 परिवर्तन स्वीकृति और प्राधिकरण के लिए संचार रिकॉर्ड करने के लिए एक परिवर्तन प्रबंधन ई–मेल समूह बनाया जा सकता है।
3. सी.एम.सी. को आवेदन से संबंधित सभी परिवर्तनों की पहचान करनी चाहिए, जिन्हें लागू करने से पहले अनुमोदन की आवश्यकता होती है।
4. सुरक्षा स्तर और एप्लिकेशन की कार्यक्षमता पर प्रभाव डालने वाले सभी परिवर्तनों को सी.एम.सी. द्वारा स्पष्ट रूप से पहचाना और अनुमोदित किया जाना चाहिए।

154. परिवर्तन अनुरोध

1. उपयोगकर्ता/सिस्टम प्रशासक द्वारा अनुरोधित सभी परिवर्तन प्राथमिकता के अनुसार सीएमसी/पीएम को प्रस्तुत किए जाने चाहिए।
2. परिवर्तन अनुरोध में निम्नलिखित विवरण होने चाहिएः
   2.1 परिवर्तन का विवरण,
   2.2 परिवर्तन का उद्देश्य या परिवर्तन का कारण,
   2.3 प्रस्तावित परिवर्तन का प्रभाव,
   2.4 रोलबैक योजना,
   2.5 परीक्षण योजना,

2.6 वैकल्पिक समाधान, यदि कोई हो, प्रदान किया जा सकता है।

155. परिवर्तन का प्रभाव विश्लेषण

1. सी.एम.सी. को अनुरोधित परिवर्तन का प्रभाव विश्लेषण करना चाहिए। निम्नलिखित मापदंडों पर विचार किया जाना चाहिए
   - 1.1 परिवर्तन की आवश्यकता,
   - 1.2 परिवर्तन का प्रभाव,
   - 1.3 परिवर्तन की प्राथमिकता,
   - 1.4 सुरक्षा निहितार्थ।

156. परिवर्तन अनुमोदन

1. परिवर्तन अनुरोध अनुमोदन व्यावसायिक आवश्यकता, प्रक्रिया में सुधार या पर्यावरण की सुरक्षा को बढ़ाने पर आधारित होना चाहिए।
2. परिवर्तन के अनुरोध को अस्वीकार कर दिया जाना चाहिए यदि यह जोखिम के शमन की गारंटी नहीं देता है।
3. सिस्टम में स्वीकृत परिवर्तनों को लागू करने के लिए एक कार्यान्वयन दल का गठन करें।
4. परिवर्तन अनुमोदन के बाद एक विस्तृत कार्यान्वयन योजना तैयार की जानी चाहिए। कार्यान्वयन योजना दस्तावेज में निम्नलिखित विवरण होने चाहिए।
   - 4.1 समय और संसाधन की आवश्यकता,
   - 4.2 पूर्व–आवश्यकताएं (यदि कोई हो),
   - 4.3 क्रियान्वयन के चरण,
   - 4.4 डाउन टाइम आवश्यकताएं,
   - 4.5 परीक्षण योजना,
   - 4.6 रोल बैक योजना।
5. सभी महत्वपूर्ण / बड़े परिवर्तनों के लिए, प्रभावित विभागों को परिवर्तन अनुसूची, प्रभाव और रखरखाव / डाउन टाइम विंडो के बारे में सूचित किया जाना चाहिए।
6. कार्यान्वयन टीम द्वारा परिवर्तन के साथ आगे बढ़ने से पहले बैकअप लिया जाना चाहिए।

157. परिवर्तन परीक्षण

1. सभी परिवर्तन प्रारंभ में एक परीक्षण प्रणाली पर किए जाने चाहिए। (जहां भी लागू हो या संभव हो)
2. कार्यान्वयन दल को एक स्टेजिंग सिस्टम (यदि उपलब्ध हो) पर रोल बैक योजना का परीक्षण भी करना चाहिए। एक बार परीक्षण के परिणामों की पुष्टि हो जाने के बाद, सी.एम.सी. को उत्पादन पर परिवर्तन के कार्यान्वयन को मंजूरी देनी चाहिए।

158. परिवर्तन कार्यान्वयन

1. कार्यान्वयन योजना के अनुसार उत्पादन प्रणाली में अनुमोदित परिवर्तन करना।
2. कार्यान्वयन के दौरान किए गए वास्तविक कदमों के विवरण वाली एक पोस्ट–कार्यान्वयन रिपोर्ट प्रस्तुत करें।
3. व्यवसाय / एप्लिकेशन धारक को यह सत्यापित करना चाहिए कि केवल परिवर्तन नियंत्रण बोर्ड द्वारा अधिकृत परिवर्तन ही लागू किए गए हैं।

159. परिवर्तन अनुश्रवण और सत्यापन

1. परिवर्तन लागू करने के बाद सिस्टम की निगरानी करें।
2. प्रभावशीलता के लिए परिवर्तन की समीक्षा की जानी चाहिए।
3. यदि परिवर्तन चिंता का कोई कारण नहीं उठाता है, तो उसे अंतिम स्वीकृति मिलनी चाहिए।
4. उत्पादन प्रणाली पर परिवर्तन के कार्यान्वयन के बाद परिवर्तन प्रभावशीलता पर उपयोगकर्ता पुष्टि प्राप्त करें।
5. भविष्य के संदर्भ और लेखा परीक्षा उद्देश्यों के लिए परिवर्तन प्रबंधन से संबंधित सभी दस्तावेजों और अभिलेखों को बनाए रखने के लिए व्यवसाय / एप्लिकेशन मालिक जिम्मेदार हैं।

160. परिवर्तन रोलबैक

1. यदि परिवर्तन को सफल नहीं माना जाता है, तो रोल बैक योजना के अनुसार परिवर्तन को वापस ले लिया जाना चाहिए।
2. एक बार रोल बैक योजना लागू हो जाने के बाद, सिस्टम को व्यवसाय / एप्लिकेशन मालिकों द्वारा सत्यापित किया जाना चाहिए।
3. व्यवसाय/एप्लिकेशन स्वामियों को परिवर्तन और रोल बैक गतिविधि का रिकॉर्ड रखना चाहिए।

161. मामूली/आपातकालीन परिवर्तन

1. संबंधित पी.एम.सी. के योजना प्रबंधकों के साथ मामूली बदलाव / तत्काल परिवर्तनों पर चर्चा की जानी चाहिए। परियोजना प्रबंधकों को यह आकलन करने और निर्णय लेने की आवश्यकता है कि क्या इसे सी.एम.सी. को प्रस्तुत किया जाना चाहिए या उनके द्वारा अनुमोदित किया जा सकता है।
2. आपात स्थिति के दौरान कंप्यूटर सिस्टम की अखंडता सुनिश्चित करने के लिए निम्नलिखित कदम उठाए जाने चाहिए:
   - 2.1 केवल उत्पादन समस्याओं को हल करने के लिए आपातकालीन सुधारों की अनुमति दें।
   - 2.2 परिवर्तन के लिए जिम्मेदार व्यक्ति को कार्यान्वित परिवर्तनों का दस्तावेजीकरण करना चाहिए।
   - 2.3 सभी आपातकालीन परिवर्तनों की समीक्षा अगले कार्य दिवस पर समीक्षक द्वारा की जानी चाहिए।

162. प्रयोज्यता

एस.डी.सी.नेटवर्क और इंटरनेट संसाधनों का उपयोग करने वाले सभी हितधारकों की इस नीति का पालन करने की जिम्मेदारी है। सिस्टम एडमिनिस्ट्रेटर और डाटा सेंटर के प्रभारी के पास इस नीति को लागू करने और यह सुनिश्चित करने की जिम्मेदारी है कि इसका पालन किया जा रहा है।

163. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–23: डाटाबेस सुरक्षा

164. प्रयोजन

इस नीति का उद्देश्य यह सुनिश्चित करना है कि यूकेएसडीसी संगठन यह सुनिश्चित करने के लिए पर्याप्त नियंत्रणों को परिभाषित, विकसित और कार्यान्वित करता है कि डाटाबेस सुरक्षा नीति में उल्लिखित आवश्यकताओं को पूरा करती है।

165. नीति वक्तव्य और उद्देश्य

इस नीति का उद्देश्य यह सुनिश्चित करना है कि सभी डाटाबेस सिस्टम को उच्च सुरक्षा के लिए स्थापित और कॉन्फ़िगर किया जाना चाहिए। यह नीति यूकेएसडीसी के सभी डाटाबेस पर लागू होती है।

166. नियंत्रण

(क) संरचना

1. एप्लिकेशन और डाटाबेस सर्वर समर्पित, संरक्षित नेटवर्क सेगमेंट पर स्थित होने चाहिए।
2. संरचना के भीतर सभी प्रणालियों को सुरक्षित रखा जाना चाहिए।
3. डाटाबेस सर्वर के ऑपरेटिंग सिस्टम को सुदृढ़ किया जाना चाहिए।

(ख) संस्थापना एवं विन्यास (Configuration)

1. डाटाबेस स्थापित करते समय, केवल आवश्यक सुविधाएँ ही स्थापित की जानी चाहिए।
2. डाटाबेस व्यवस्थापक पासवर्ड रिक्त नहीं होना चाहिए।
3. डाटाबेस/सुरक्षा कॉन्फ़िगरेशन और सेटिंग्स को सुरक्षित स्थान पर रिकॉर्ड और संग्रहीत किया जाना चाहिए।
4. किसी भी दुर्भावनापूर्ण गतिविधि की स्थिति में, डाटाबेस व्यवस्थापक वर्तमान सेटिंग को तेज़ी से पुनर्स्थापित कर सकता है।
5. संस्थापन मीडिया की प्रतियां ऑफ–साइट संग्रहित की जानी चाहिए।

(ग) फ़ाइल सिस्टम सुरक्षा

1. डाटाबेस सिस्टम ऑपरेटिंग सिस्टम फाइलों में कॉन्फ़िगरेशन सेटिंग्स और डाटा सहित सभी सूचनाओं को संग्रहीत करता है।
   1.1 इन फाइलों को ऑपरेटिंग सिस्टम स्तर की अनुमतियों द्वारा संरक्षित किया जाना चाहिए।
   1.2 एप्लिकेशन स्वामी को यह सुनिश्चित करना चाहिए कि इन फ़ाइलों पर उपयुक्त एक्सेस अनुमतियां विशेष एप्लिकेशन के लिए सुरक्षित कॉन्फ़िगरेशन दस्तावेज़ में शामिल हैं।

1.3 डाटाबेस व्यवस्थापकों को यह सुनिश्चित करना चाहिए कि ये फाइलें एप्लिकेशन के लिए सुरक्षित कॉन्फिगरेशन दस्तावेज़ के अनुसार स्थापित करके सुरक्षित हैं।

1.4 प्रारंभिक कार्यान्वयन के दौरान, एप्लिकेशन स्वामी को स्थापना रिपोर्ट को सत्यापित करना चाहिए कि सभी सिस्टम सुरक्षित रूप से कॉन्फिगर किए गए हैं।

2. डाटाबेस का बैकअप, बैकअप प्रक्रिया के अनुसार लिया जाना चाहिए। बैकअप मीडिया की प्रतियां ऑफ–साइट संग्रहित की जानी चाहिए।

(घ) उपयोगकर्ता प्रमाणीकरण:

1. सभी डाटाबेस उपयोगकर्ताओं को पहुँच प्रदान करने से पहले प्रमाणित किया जाना चाहिए।

1.1 उपयोगकर्ता आईडी और पासवर्ड प्रदान करने के बाद ही पहुंच प्रदान की जानी चाहिए।

1.2 डिफॉल्ट पासवर्ड वाला या बिना पासवर्ड वाला कोई भी अकाउंट नहीं होना चाहिए।

2. सभी डाटाबेस उपयोगकर्ताओं के पास एक विशिष्ट उपयोगकर्ता–आईडी होना चाहिए। उपयोगकर्ता खातों को साझा नहीं किया जाना चाहिए।

2.1 उदाहरण के लिए यदि दो उपयोगकर्ताओं को डाटाबेस पर बैकअप विशेषाधिकारों की आवश्यकता होती है, तो दोनों उपयोगकर्ताओं को एक खाते को साझा करने के बजाय बैकअप विशेषाधिकारों वाले दो अलग–अलग खाते बनाए जाने चाहिए।

2.2 डाटाबेस SQL–इंजेक्शन हमलों के लिए असुरक्षित नहीं होना चाहिए, सर्वर और क्लाइंट दोनों को सत्यापन करना चाहिए।

(ङ) नवीन उपयोगकर्ता प्रावधान

3. डाटाबेस में उपयोगकर्ता खाते केवल एप्लिकेशन एक्सेस, डाटाबेस बैकअप और डाटाबेस रखरखाव / अनुकूलन गतिविधियों के लिए बनाए जाने चाहिए।

4. नए उपयोगकर्ता निर्माण को एक परिभाषित नामकरण परंपरा मानक का पालन करना चाहिए।

5. सभी खातों को केवल विशिष्ट एप्लिकेशन द्वारा उपयोग किए जाने वाले डाटाबेस टेबल तक पहुंच प्रदान की जानी चाहिए। एप्लिकेशन विशिष्ट खातों की अन्य तालिकाओं और कॉन्फिगरेशन मापदंडों तक पहुंच नहीं होनी चाहिए।

5.1 अधिकांश एप्लिकेशन डाटाबेस तक पहुंचने के लिए सभी एप्लिकेशन उपयोगकर्ताओं के लिए एक सामान्य खाते का उपयोग करते हैं। इस मामले में इस एप्लिकेशन एक्सेस के लिए डाटाबेस खाते में उच्च विशेषाधिकार होंगे। सुनिश्चित करें कि यह डाटाबेस के लिए अंतर्निहित व्यवस्थापक खाता नहीं है। एक नया खाता बनाएं और एप्लिकेशन को कार्य करने के लिए आवश्यक सभी विशेषाधिकार आवंटित करें।

5.2 कुछ एप्लिकेशन में प्रत्येक संबंधित एप्लिकेशन उपयोगकर्ता के लिए एक डाटाबेस यूजर–आईडी होता है। इन खातों को जानने की आवश्यकता के आधार पर डाटाबेस में एक्सेस अधिकार दिए जाने चाहिए।

6. डाटाबेस में नए उपयोगकर्ता खाते व्यवसाय / एप्लिकेशन स्वामी से अनुमोदन के बाद ही बनाए जाने चाहिए।

7. नए उपयोगकर्ता का निर्माण और उपयोगकर्ता विशेषाधिकार प्रदान करना अलग–अलग व्यक्तियों द्वारा किया जाना चाहिए। डाटाबेस व्यवस्थापक के पास डाटाबेस में एक खाता होना चाहिए जिसमें उपयोगकर्ता खाते बनाने के लिए विशेषाधिकार हों। डाटाबेस व्यवस्थापक को बिना किसी विशेषाधिकार के डाटाबेस में खाता बनाना चाहिए और नए उपयोगकर्ता को स्वीकृत विशेषाधिकार आवंटित करना चाहिए।

   7.1 यदि डाटाबेस एप्लिकेशन उपयोगकर्ता निर्माण और विशेषाधिकार आवंटन कार्यों को अलग करने की सुविधा प्रदान नहीं करता है, तो एप्लिकेशन स्वामी को नए उपयोगकर्ता प्रावधान में कर्तव्यों के पृथक्करण को प्राप्त करने के लिए वैकल्पिक तकनीकी नियंत्रण लागू करना चाहिए। (उदाहरण के लिए एक अलग सर्वर पर लॉग इन किया गया और खाता बनाने वाले के अलावा किसी अन्य व्यक्ति द्वारा जांच की गई)

   7.2 यदि किसी उपयोगकर्ता को खाता बनाने के बाद अतिरिक्त विशेषाधिकारों की आवश्यकता होती है, तो एप्लिकेशन स्वामी को अतिरिक्त विशेषाधिकारों के अनुरोध को स्वीकार करना चाहिए और डाटाबेस व्यवस्थापक को विशेषाधिकार आवंटित करना चाहिए।

8. उपयोगकर्ता अधिकारों को कम से कम विशेषाधिकार के सिद्धांत के आधार पर आवंटित किया जाना चाहिए। प्रयोक्ता अधिकार आवश्यकता और करने की आवश्यकता के आधार पर होना चाहिए।

9. विशेषाधिकार प्राप्त और सामान्य (गैर–विशेषाधिकार प्राप्त) गतिविधियों को करने के लिए एक ही उपयोगकर्ता को अलग उपयोगकर्ता आईडी आवंटित की जा सकती हैं।

   9.1 उदाहरण के लिए यदि डाटाबेस व्यवस्थापक उपयोगकर्ता अधिकारों को सत्यापित करने जैसे कार्य करता है जिसके लिए प्रशासनिक विशेषाधिकारों की आवश्यकता नहीं होती है, तो उसके पास एक अलग खाता हो सकता है जिसमें केवल सीमित पहुंच हो। यह डाटाबेस प्रशासकों द्वारा आकस्मिक त्रुटियों के जोखिम को सीमित करेगा और ऑडिटिंग उद्देश्यों में भी मदद करेगा।

   9.2 असंगत विशेषाधिकार (अनुरोध और अनुमोदन भूमिकाएं) किसी एकल उपयोगकर्ता आईडी को नहीं सौंपे जाने चाहिए।

(च) अकाउंट नीति

1. डाटाबेस प्रशासन के लिए जिम्मेदार डाटाबेस व्यवस्थापक को निम्न खाता नीति सेटिंग्स को लागू करने के लिए डिफॉल्ट उपयोगकर्ता प्रोफाइल को संशोधित करना चाहिए।

   1.1 डाटाबेस को 8 वर्णों की न्यूनतम पासवर्ड लंबाई लागू करनी चाहिए।

   1.2 पासवर्ड हिस्ट्री को मेंटेन करना चाहिए। अंतिम 5 पासवर्ड प्रयोग करने योग्य नहीं होने चाहिए।

   1.3 खाता लॉकआउट सुविधा सक्षम की जानी चाहिए।

      1.3.1 5 विफल लॉगिन प्रयासों के बाद डाटाबेस को उपयोगकर्ता खाते को लॉक करना चाहिए।

      1.3.2 खाते को अनलॉक करने के लिए केवल डाटाबेस व्यवस्थापक के पास विशेषाधिकार होने चाहिए।

1.4 पासवर्ड की समाप्ति 90 दिनों पर सेट की जानी चाहिए।

1.5 डाटाबेस व्यवस्थापक को यह सुनिश्चित करने के लिए ज़िम्मेदार होना चाहिए कि डाटाबेस तक पहुँचने के लिए एप्लिकेशन द्वारा उपयोग किए जाने वाले खाते के लिए पासवर्ड समय–समय पर बदला जाता है।

1.6 एप्लिकेशन को इस पासवर्ड को बदलने के लिए एक तंत्र प्रदान करना चाहिए।

1.7 यह पासवर्ड एप्लिकेशन स्रोत कोड का हिस्सा नहीं होना चाहिए (अर्थात एप्लिकेशन में हार्ड कोडेड नहीं किया गया है)।

2. सभी विक्रेता द्वारा प्रदत्त डिफॉल्ट उपयोगकर्ता आईडी का नाम बदल दिया जाएगा या अक्षम कर दिया जाएगा या पासवर्ड बदल दिया जाएगा। उपयोगकर्ता खाते जो डाटाबेस की डिफॉल्ट स्थापना का हिस्सा हैं, लेकिन सामान्य संचालन के लिए आवश्यक नहीं हैं, उन्हें हटा दिया जाना चाहिए।
उदाहरण के लिए, Oracle संस्थापन के दौरान कुछ डिफॉल्ट खाते डिफॉल्ट पासवर्ड के साथ बनाए जाते हैं। इनमें से कुछ उपयोगकर्ता नाम–पासवर्ड संयोजन TRACESVR-TRACE, SYSADM-SYSADM, SCOTT-TIGER हैं।

3. उपयोगकर्ता आईडी में उपयोगकर्ता के विशेषाधिकार स्तर का कोई संकेत नहीं देना चाहिए। उदाहरण के लिए, उपयोगकर्ता–आईडी जैसे 'सुपरवाइजर', 'डाटाबेस–एडमिन' आदि से बचा जाना चाहिए।

(घ) डाटा एकीकरण

1. समवर्ती उपयोगकर्ता मोड में डाटा का एकीकरण को रिकॉर्ड लॉकिंग या दो–चरण लॉकिंग / प्रतिबद्ध सुविधाओं के माध्यम से डाटाबेस में डिज़ाइन किया जाना चाहिए।

2. डाटा की संदर्भात्मक एकीकरण को डाटाबेस डिज़ाइन में बनाए रखा जाना चाहिए और इसमें कैस्केडिंग अपडेट और कैस्केडिंग डिलीट शामिल होना चाहिए, यह सुनिश्चित करने के लिए कि लिंक की गई तालिका में किए गए परिवर्तन प्राथमिक तालिका में परिलक्षित होते हैं।

(ङ) लॉगिंगः

1. सिस्टम के दुरुपयोग को ट्रैक करने के लिए लॉगिंग को सक्षम किया जाना चाहिए। ऑडिट डाटाबेस प्रशासकों को महत्वपूर्ण घटनाओं की निगरानी करने में सक्षम बनाता है और यह दुर्भावनापूर्ण पहुंच के प्रयासों के प्रति एक प्रारंभिक चेतावनी है। लॉग ऑडिट ट्रेल प्रदान करते हैं और धोखाधड़ी की स्थिति में दुर्भावनापूर्ण उपयोगकर्ताओं को ट्रैक करने में महत्वपूर्ण भूमिका निभाते हैं। डाटाबेस निम्नलिखित सहित सभी सुरक्षा संबंधी घटनाओं को लॉग करने में सक्षम होना चाहिएः

1.1 उपयोगकर्ता खाता प्रबंधन,

1.2 उपयोगकर्ता विशेषाधिकार परिवर्तन,

1.3 उपयोगकर्ता लॉगिन/लॉगआउट समय,

1.4 डाटाबेस कॉन्फ़िगरेशन में परिवर्तन,

1.5 प्रमाणीकरण विफलता।

2. एप्लिकेशन स्वामी को डाटाबेस लॉग फाइलों के लिए अवधारण अवधि निर्धारित करनी चाहिए। एप्लिकेशन स्वामी को यह सुनिश्चित करना चाहिए कि प्रतिधारण अवधि रिकॉर्ड प्रतिधारण के लिए यूकेएसडीसी की नीति के अनुरूप है।
3. एप्लिकेशन स्वामियों को यह सुनिश्चित करने की आवश्यकता है कि उपयुक्त लॉगिंग विधियाँ, जो टाइम स्टैम्प के साथ उपयोगकर्ता आईडी को कैप्चर करती हैं, डाटाबेस के भीतर सुरक्षा संबंधी घटनाओं के बारे में आवश्यक जानकारी प्रदान करने के लिए सक्षम हैं।

(झ) पैच अद्यतन

1. डाटाबेस प्रशासन के लिए जिम्मेदार डाटाबेस व्यवस्थापक को यह सुनिश्चित करना चाहिए कि डाटाबेस एप्लिकेशन को नवीनतम सुरक्षा पैच और हॉट फिक्स के साथ अद्यतन किया गया है।
2. सिस्टम एडमिनिस्ट्रेटर नए जारी किए गए पैच को ट्रैक करने और संबंधित एप्लिकेशन मालिकों और डाटाबेस एडमिनिस्ट्रेटर को इसे वितरित करने के लिए जिम्मेदार है।

(ञ) भौतिक सुरक्षा

1. उस स्थान तक भौतिक पहुंच जहां सर्वर स्थित हैं, नियंत्रित, निगरानी और अधिकृत लोगों तक सीमित होनी चाहिए।
2. डाटाबेस में संग्रहीत डाटा को आमतौर पर यूकेएसडीसी के लिए महत्वपूर्ण माना जाता है। डाटाबेस रखने वाले सर्वर का स्थान लॉक और नियंत्रित कमरे में होना चाहिए। इसमें अन्य भौतिक सुरक्षा नियंत्रण जैसे अग्नि शमन प्रणाली, निर्बाध विद्युत आपूर्ति और तापमान और आर्द्रता नियंत्रण प्रणाली शामिल हैं।

167. प्रयोज्यता

एस.डी.सी. नेटवर्क का उपयोग करने वाले सभी हितधारकों की इस नीति का पालन करने की जिम्मेदारी है। डाटा सेंटर के प्रभारी के पास इस नीति को लागू करने और यह सुनिश्चित करने की जिम्मेदारी है कि इसका पालन किया जा रहा है।

168. प्रवर्तन एवं व्याख्याः

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–24: डेस्कटॉप सुरक्षा

169. प्रयोजन

इस नीति का प्रयोजन यूकेएसडीसी, आईटीडीए के स्वामित्व और/या संचालित आंतरिक डेस्कटॉप उपकरणों के आधार विन्यास के लिए मानकों को स्थापित करना है। इस नीति के प्रभावी क्रियान्वयन से आईटीडीए के स्वामित्व वाली सूचना और प्रौद्योगिकी तक अनधिकृत पहुंच कम होगी।

170. नीति कथन और उद्देश्य

यह नीति यूकेएसडीसी, आईटीडीए के स्वामित्व और/या संचालित और किसी भी आईटीडीए के स्वामित्व वाले आंतरिक नेटवर्क डोमेन के अंतर्गत पंजीकृत डेस्कटॉप उपकरण पर लागू होती है। यह नीति विशेष रूप से आंतरिक नेटवर्क पर उपकरणों के लिए है।

171. नियंत्रण

1. यूकेएसडीसी में तैनात क्लाइंट मशीनों को नियंत्रित वातावरण में डाटा को संसाधित करना चाहिए, आसानी से प्रबंधनीय होना चाहिए और डाटा को संसाधित करने के लिए पर्याप्त स्तर तक सुरक्षित होना चाहिए।
2. क्लाइंट मशीनों को यूकेएसडीसी डाटा स्थायी रूप से नहीं रखना चाहिए। जहां भी संभव हो केन्द्रीय सर्वरों को इस डाटा को रखना चाहिए, जिसे आसानी से पुनर्प्राप्त किया जा सकता है, यदि क्लाइंट मशीन लुप्त हो जाती है, क्षतिग्रस्त हो जाती है या आम तौर पर अनुपलब्ध होती है।
3. यूकेएसडीसी डाटा को क्लाइंट मशीनों को अनियंत्रित तरीके से नहीं छोड़ना चाहिए।
4. यूकेएसडीसी डाटा के अनधिकृत इलेक्ट्रॉनिक निष्कासन को कम करने के लिए विशेष रूप से हार्डवेयर को कॉन्फिगर किया जाना चाहिए।
5. उचित पहुंच विशेषाधिकार को परिभाषित किया जाना चाहिए, सभी को किसी भी फोल्डर को पूर्ण अनुमति नहीं दी जानी चाहिए।
6. क्लाइंट मशीनों को केवल उपयोगकर्ता द्वारा आवश्यक एप्लिकेशन प्रदान करने के लिए कॉन्फिगर किया जाना चाहिए, उनके काम को पूरा करने के लिए कम से कम विशेषाधिकार की आवश्यकता होती है। जहां भी संभव हो 'थिन क्लाइंट एप्लिकेशन' को कम से कम किया जाना चाहिए, वेब/ब्राउज़र–आधारित एप्लिकेशन पसंदीदा क्लाइंट होने चाहिए।
7. उपयोगकर्ताओं को अपने क्लाइंट मशीनों पर बिना लाइसेंस वाले सॉफ़्टवेयर या अस्वीकृत हार्डवेयर स्थापित करने की अनुमति नहीं दी जानी चाहिए।
8. क्लाइंट मशीन के ऑपरेटिंग सिस्टम को जारी होने पर नवीनतम सर्विस पैक और पैच के साथ अद्यतन किया जाना चाहिए।
9. वर्कस्टेशन को निम्नलिखित के रूप में वर्गीकृत और प्रोफाइल किया जाना चाहिए:
   (क) स्टाफ वर्कस्टेशन,
   (ख) विभाग वर्कस्टेशन,
   (ग) समर्थन और विकास वर्कस्टेशन,

(घ) क्रिटिकल/सेंसिटिव एरिया वर्कस्टेशन,

(ङ) प्रबंधन वर्कस्टेशन / लैपटॉप।

1. एक्टिव डायरेक्ट्री पर स्पेशलाइज्ड ग्लोबल पॉलिसी ऑब्जेक्ट (जीपीओ) बनाए जाने चाहिए।
2. क्लाइंट मशीनों पर केवल लाइसेंस प्राप्त सॉफ़्टवेयर स्थापित किया जाना चाहिए और सॉफ़्टवेयर का नियमित रूप से ऑडिट किया जाना चाहिए।
3. क्लाइंट मशीन पर केवल NTFS विभाजन बनाया जाना चाहिए।
4. क्लाइंट मशीनों के लिए सशक्त पासवर्ड नीति लागू करें:
   (क) पासवर्ड हिस्ट्री लागू करें – 5,
   (ख) अधिकतम पासवर्ड आयु – 45,
   (ग) न्यूनतम पासवर्ड आयु – 0,
   (घ) पासवर्ड की न्यूनतम लंबाई – 8,
   (ङ) पासवर्ड को जटिलता के अनुरूप होना चाहिए – सक्षम,
   (च) खाता लॉकआउट अवधि – 30 मिनट,
   (छ) खाता लॉकआउट सीमा – 5,
   (ज) खाता लॉकआउट काउंटर रीसेट करें – 30 मिनट के बाद।

I. सभी क्लाइंट मशीनों पर ऑडिटिंग सक्षम होनी चाहिए।

II. सभी क्लाइंट मशीनों को यूकेएसडीसी डोमेन पर सेट किया जाना चाहिए

III. समय को एडी सर्वर के साथ सिंक्रनाइज़ किया जाना चाहिए और समय क्षेत्र (जीएमटी +05: 30) चेन्नई, कोलकाता, मुंबई, नई दिल्ली होना चाहिए।

IV. स्क्रीन सेवर पासवर्ड सभी क्लाइंट मशीनों पर सक्षम होना चाहिए

V. मानक स्क्रीन सेवर और डेस्कटॉप को कॉन्फ़िगर किया जाना चाहिए

VI. सभी क्लाइंट मशीनों पर एंटी–वायरस सॉफ़्टवेयर स्थापित किया जाना चाहिए और नियमित अपडेट कॉन्फ़िगर किए जाने चाहिए।

VII. एमएसएन और याहू मैसेंजर, चैट एप्लिकेशन और म्यूजिक सॉफ्टवेयर के साथ सभी क्लाइंट मशीनों को स्थापित नहीं किया जाना चाहिए।

VIII. यूकेएसडीसी नेटवर्क से कनेक्ट होने के दौरान वायरलेस लैन/डायलअप/ब्लूटूथ/इन्फ्रारेड और अन्य नेटवर्किंग को अक्षम कर दिया जाना चाहिए।

172. बाह्य उपकरण

निम्नलिखित मदों को उपयुक्त के रूप में अक्षम, हटा या प्रतिस्थापित करें:–

(क) लिखने योग्य (या फिर से लिखने योग्य) मीडिया उपकरण,

(ख) फ्लॉपी / टेप ड्राइव,

(ग) यूएसबी / सीरियल पोर्ट,

(घ) ब्लूटूथ/वायरलेस लैन/इन्फ्रारेड,

(ङ) मोडेम जब तक कि क्लाइंट मशीन पोर्टेबल न हो।

173. मानक एप्लीकेशन

कम से कम विशेषाधिकार सुनिश्चित करने के लिए, क्लाइंट मशीनों को केवल निम्नलिखित एप्लीकेशन के साथ स्थापित किया जाना चाहिए:–

(क) सिस्टम यूटिलिटीज,

(ख) एमएस ऑफिस (घटक: एक्सेल, वर्ड, पावरपॉइंट, आउटलुक, आदि),

(ग) एडोब एक्रोबेट रीडर,

(घ) विनजिप,

(ङ) एंटीवायरस अनुप्रयोग,

(च) एंटी स्पाइवेयर,

(छ) क्लाइंट एप्लीकेशन।

(i) क्लाइंट मशीनों पर केवल स्वीकृत सॉफ्टवेयर चलाने की अनुमति देने के लिए ग्लोबल पॉलिसी ऑब्जेक्ट (जीपीओ) का उपयोग किया जाना चाहिए।

(ii) किसी भी नए सॉफ्टवेयर इंस्टॉलेशन अनुरोध को आईटी विभाग द्वारा अनुमोदित किया जाना चाहिए और इसे स्वीकृत करने से पहले आई.एस.ओ. द्वारा संबद्ध जोखिम का मूल्यांकन किया जाना चाहिए।

(iii) सभी गोपनीय अभिलेखों को एक केन्द्रीय सर्वर में संग्रहीत करने की सिफारिश की जाती है और नियमित रूप से बैकअप लिया जाना चाहिए।

(iv) सभी क्लाइंट मशीनों का निस्तारण किया जाना चाहिए, सभी डाटा को साफ किया जाना चाहिए, मीडिया उपकरणों को एक गैर–स्वरूपित स्थिति में लौटाना चाहिए। डाटा को एक सुरक्षित वाइप या डिलीट मैकेनिज्म का उपयोग करके मिटा दिया जाना चाहिए।

(v) यूकेएसडीसी कर्मचारियों के लिए पुनः उपयोग की जाने वाली क्लाइंट मशीनों को प्रारूपित किया जाना चाहिए और डेस्कटॉप नीति के लिए पूरी तरह से कॉन्फिगर किया जाना चाहिए। पिछले मालिकों से संबंधित सभी डाटा को हटा दिया जाना चाहिए या भविष्य में उपयोग के लिए संग्रहीत किया जाना चाहिए, जिसमें उचित पहुंच नियंत्रण हो।

(vi) सभी यूकेएसडीसी क्लाइंट मशीनों के लिए विंडोज एक्सपी प्रोफेशनल की क्लीन इंस्टालेशन की जानी चाहिए।

(vii) क्लाइंट मशीन बूट को केवल उसकी प्राथमिक हार्ड ड्राइव से सुनिश्चित करने के लिए BIOS को सेट किया जाना चाहिए।

(viii) क्लाइंट मशीनों पर स्थापित ऑपरेटिंग सिस्टम और अन्य एप्लिकेशन के लिए लाइसेंसिंग को ट्रैक किया जाना चाहिए।

174. प्रयोज्यता

यह नीति यूकेएसडीसी के सभी हितधारकों के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की गई है।

175. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–25: फायरवॉल

176. प्रयोजन

इस नीति का उद्देश्य यह सुनिश्चित करना है कि महत्वपूर्ण मशीनों तक सभी पहुंच फायरवॉल द्वारा मान्य है।

177. नीति कथन और उद्देश्य

यह नीति उन सभी उपयोगकर्ताओं पर लागू होती है जो वी.पी.एन. के माध्यम से बाह्य नेटवर्क से यूकेएसडीसी नेटवर्क से जुड़ रहे हैं।

178. नियंत्रण

(क) फायरवॉल टीम

1. फायरवॉल/सिस्टम एडमिनिस्ट्रेटर फायरवॉल और उसके नियम आधार की स्थापना, कॉन्फिगरेशन और रखरखाव के लिए जिम्मेदार है। फायरवॉल/सिस्टम एडमिनिस्ट्रेटर सी.आई.एस.ओ. को रिपोर्ट करेगा।

1.1 सभी नियम आधार परिवर्तनों को सी.आई.एस.ओ. द्वारा अनुमोदित किया जाना चाहिए और उसके बाद ही फायरवॉल पर लागू किया जाना चाहिए।

(ख) फायरवॉल मशीन की सुरक्षा

1. फायरवॉल को भौतिक रूप से और साथ ही तार्किक रूप से सुरक्षित किया जाना चाहिए।
2. फायरवॉल सिस्टम में ऐसी कोई अतिरिक्त सेवा नहीं होनी चाहिए जिसे दूरस्थ रूप से एक्सेस किया जा सके। फायरवॉल मशीन पर चलने वाली एस.एम.टी.पी., डी.एन.एस. जैसी कोई अतिरिक्त सेवा हमलावरों को सेवा से जुड़ी कमजोरियों का फायदा उठाकर फायरवॉल से समझौता करने का अवसर प्रदान करेगी।
3. फायरवॉल मशीन को केवल अधिकृत कर्मियों तक ही पहुंच के साथ एक नियंत्रित भौतिक पहुंच वातावरण में रखा जाना चाहिए।
4. किसी भी अप्रयुक्त भौतिक इंटरफेस को फायरवॉल पर अक्षम/डी–एक्टिवेट किया जाना चाहिए।
5. सुरक्षित नेटवर्क आरेख को प्रलेखित और अनुमोदित किया जाना चाहिए।
6. फायरवॉल प्लेसमेंट स्वीकृत सुरक्षित नेटवर्क संरचना आरेख के अनुसार होना चाहिए।

(ग) फायरवॉल सेगमेंट

1. फायरवॉल को जोखिम स्तरों के आधार पर नेटवर्क को विभाजित करना चाहिए।

1.1 इंटरनेट का सामना करने वाले सर्वर और बाह्य पार्टियों जैसे एक्स्ट्रानेट आदि द्वारा एक्सेस किए गए सर्वर एक अलग सेगमेंट (डी–मिलिटरीकृत जोन – डीएमजेड) पर होने चाहिए।

1.2 यूटिलिटी सर्वर जैसे एवी, एक्टिव डायरेक्ट्री, प्रॉक्सी आदि दूसरे सेगमेंट पर होने चाहिए।

1.3 एप्लिकेशन और डाटाबेस सर्वर को संरक्षित सेगमेंट पर रखकर संरक्षित किया जाना चाहिए। इस सेगमेंट के पास केवल उपयोगकर्ताओं से आवश्यक पहुंच होनी चाहिए।

2. यूकेएसडीसी नेटवर्क और गैर–यूकेएसडीसी (पार्टनर या वेंडर) नेटवर्क के बीच हर कनेक्शन को फायरवॉल द्वारा नियंत्रित किया जाएगा।

3. सर्वर और डेस्कटॉप अपने जोखिम के आधार पर अलग–अलग सेगमेंट में होने चाहिए।

3.1 उपयोगकर्ता सेगमेंट को फायरवॉल द्वारा अलग किया जाना चाहिए। केवल डेस्कटॉप और लैपटॉप को ही इस सेगमेंट से कनेक्ट होना चाहिए। कर्मचारियों, विक्रेताओं और तीसरे पक्ष के ठेकेदारों आदि को इस सेगमेंट का उपयोग करना चाहिए।

(घ) फायरवॉल रूल बेस निर्माण

1. फायरवॉल/सिस्टम एडमिनिस्ट्रेटर तैनाती से पहले फायरवॉल रूल बेस के डिजाइन और परीक्षण के लिए जिम्मेदार है।

2. फायरवॉल/सिस्टम एडमिनिस्ट्रेटर को रूल बेस डिजाइन करने के लिए संबंधित एप्लिकेशन के मालिक/डेवलपर से जरूरी इनपुट्स लेने चाहिए।

3. फायरवॉल रूल बेस को लक्ष्य मशीन पर केवल आवश्यक पोर्ट तक पहुंच की अनुमति देनी चाहिए।

4. रूल बेस में स्रोत फील्ड जहां भी संभव हो, विशिष्ट आई.पी. पते/सबनेट पते/उपयोगकर्ता नाम तक ही सीमित होना चाहिए।

5. उन एप्लिकेशन के मामले में जहां व्यक्तिगत आई.पी. पते/सबनेट की संख्या बहुत बड़ी है, तो रूल बेस को अधिक प्रबंधनीय बनाने के लिए स्रोत पते को सामान्य बनाया जा सकता है।

6. रूल बेस में स्टेल्थ रूल होना चाहिए।

6.1 स्टील्थ नियम फायरवॉल सिस्टम तक पहुँच को प्रतिबंधित करता है

6.2 रूल बेस में इस नियम की नियुक्ति महत्वपूर्ण है और इसे सभी प्रशासनिक और वी.पी.एन. एक्सेस नियमों के बाद फायरवॉल में रखा जाना चाहिए।

7. फायरवॉल के पास स्पष्ट रूप से अनुमत सभी पहुंच को अस्वीकार करने का नियम होना चाहिए।

8. परिनियोजन से पहले रूल बेस को सी.आई.एस.ओ. और एप्लिकेशन स्वामी/डेवलपर द्वारा अनुमोदित किया जाना चाहिए।

9. फायरवॉल/सिस्टम एडमिनिस्ट्रेटर को यह सुनिश्चित करना चाहिए कि जहां भी संभव हो सिस्टम सूचना को ब्लॉक करने के लिए फायरवॉल का उपयोग किया जाना चाहिए।

10. फायरवॉल को एप्लिकेशन–स्तरीय फिल्टरिंग भी करनी चाहिए ताकि यह सुनिश्चित हो सके कि फायरवॉल से गुजरने वाले एप्लिकेशन से संबंधित डाटा में दुर्भावनापूर्ण डाटा नहीं है।

11. बाहरी नेटवर्क से सभी उपयोगकर्ता एक्सेस को फायरवॉल पर प्रमाणित किया जाना चाहिए।

12. यूकेएसडीसी नेटवर्क तक पहुंचने वाले दूरस्थ उपयोगकर्ता को यह सुनिश्चित करना चाहिए कि उनका सिस्टम यूकेएसडीसी की सुरक्षा नीति का पालन कर रहा है।

(ङ) फायरवॉल रूल बेस परिवर्तन

1. फायरवॉल के उत्पादन में जाने के बाद, सुरक्षा स्तर को बनाए रखने के लिए, उचित प्राधिकरण के बाद रूल बेस में सभी परिवर्तन किए जाने चाहिए।
   - 1.1 किसी भी एक्सेस आवश्यकता के लिए उपयोगकर्ता को एप्लिकेशन स्वामी / डेवलपर से संपर्क करना चाहिए।
   - 1.2 एप्लिकेशन के मालिक/विभाग प्रमुख को अनुरोध को मान्य करना चाहिए, उपयोगकर्ता के अनुरोध को विशिष्ट आई.पी. पते और पोर्ट नंबरों में अनुवाद करना चाहिए और इसे सिस्टम/फायरवॉल व्यवस्थापक को भेजना चाहिए।
   - 1.3 सिस्टम/फायरवॉल व्यवस्थापक को परिवर्तन प्रबंधन समिति (सीएमसी) को अनुरोध देना चाहिए।
   - 1.4 परिवर्तन प्रबंधन समिति सुरक्षा निहितार्थ और आवश्यकता के आधार पर अनुरोध को स्वीकृत या संशोधित या अस्वीकार करेगी।
   - 1.5 परिवर्तन प्रबंधन समिति सिस्टम / फायरवॉल एडमिनिस्ट्रेटर को मंजूरी मिलने पर परिवर्तन को लागू करने के लिए कहेगी।
   - 1.6 परिवर्तन प्रबंधन समिति एक सत्यापनकर्ता को फायरवॉल रूल बेस परिवर्तन को सत्यापित करने के लिए अधिकृत करेगी।
2. परिनियोजन से पहले नियमों में सभी परिवर्तनों का परीक्षण किया जाना चाहिए।
3. परिवर्तनों का परीक्षण या तो स्टैंडबाय फायरवॉल (यदि यह उपलब्ध है) पर या स्वयं उत्पादन फायरवॉल पर आवश्यकता से अधिक पहुँच को सक्षम करके और लॉगिंग को सक्षम करके किया जा सकता है।
4. लॉग का उपयोग सटीक पोर्ट आवश्यकताओं को सत्यापित करने के लिए किया जा सकता है।
5. फायरवॉल लॉग के आधार पर पोर्ट्स को ठीक करने की गतिविधि को जल्दी से पूरा किया जाना चाहिए क्योंकि इस समय के दौरान अनधिकृत पहुंच का खतरा होता है।

179. प्रशासनिक पहुंच

1. प्रशासनिक उद्देश्यों के लिए फायरवॉल का उपयोग करने वाले उपयोगकर्ताओं को आवश्यकता के आधार पर अधिकार दिए जाने चाहिए और उन्हें सी.एम.सी. द्वारा अनुमोदित किया जाना चाहिए।
2. रूल बेस संशोधन, फायरवॉल–उपयोगकर्ता खाता प्रबंधन, फायरवॉल–व्यवस्थापक खाता प्रबंधन और लॉग अनुश्रवण सहित गतिविधियों के लिए फायरवॉल एप्लिकेशन तक प्रशासनिक पहुंच आवश्यक है।
3. आवश्यकता के आधार पर फायरवॉल पर बनाए गए उपयोगकर्ता को एक्सेस विशेषाधिकार प्रदान किए जाने चाहिए और सी.एम.सी. द्वारा अनुमोदित होना चाहिए।
4. फायरवॉल व्यवस्थापन कार्यक्रमों तक पहुँच एन्क्रिप्टेड चैनल के माध्यम से होनी चाहिए। यदि फायरवॉल सॉफ़्टवेयर स्वयं यह सुविधा प्रदान नहीं करता है, तो इस उद्देश्य के लिए एसएसएल जैसे अतिरिक्त तंत्र का उपयोग किया जाना चाहिए।
5. फायरवॉल तक तार्किक पहुँच सिस्टम/फायरवॉल व्यवस्थापक तक सीमित होनी चाहिए और सी.आई.एस.ओ. द्वारा अधिकृत होना चाहिए।

6. किसी भी अप्रयुक्त उपयोगकर्ता या सिस्टम खाते को हटा दिया जाना चाहिए या अक्षम कर दिया जाना चाहिए।

180. रूल अनुश्रवण

एक्सेस प्रतिबंध लागू करते समय फायरवॉल को नेटवर्क स्रोत पता, नेटवर्क गंतव्य पता, प्रोटोकॉल सत्र और कुछ हद तक एप्लिकेशन उपयोग की जांच करनी चाहिए।

181. लॉगिंग

1. व्यवस्थापकों द्वारा किए गए परिवर्तनों को ट्रैक करने के लिए लॉगिंग को फायरवॉल पर सक्षम किया जाना चाहिए।
2. यह सुनिश्चित करने के लिए लॉगिंग को सक्षम करने की आवश्यकता है कि सभी महत्वपूर्ण पहुंच को ट्रैक किया गया है।
3. प्रशासनिक पहुँच को सक्षम करने वाले नियमों के लिए लॉगिंग सक्षम की जानी चाहिए।
4. सामान्य उपयोगकर्ता पहुँच के लिए लॉगिंग सक्षम नहीं की जानी चाहिए।
5. फायरवॉल नियम आधार प्रतिबंधों को बायपास करने के सभी प्रयासों को लॉग किया जाना चाहिए अर्थात अंतिम नियम के लिए लॉगिंग को सक्षम किया जाना चाहिए जो अन्य नियमों द्वारा स्पष्ट रूप से अनुमत सभी एक्सेस को अवरुद्ध करता है।
6. यदि NetBIOS प्रसारण जैसी ज्ञात सेवाएं हैं जो बड़ी मात्रा में लॉग प्रविष्टियां उत्पन्न करती हैं, तो बिना लॉगिंग के इस यातायात को अवरुद्ध करने के लिए अंतिम नियम के ऊपर एक अलग नियम जोड़ा जाना चाहिए।
7. सिस्टम/फायरवॉल व्यवस्थापक और सी.आई.एस.ओ. को फायरवॉल या नेटवर्क पर महत्वपूर्ण घटनाओं या उल्लंघनों की चेतावनी को कॉन्फिगर करें।
8. वास्तविक समय में बैकअप लॉग के लिए द्वितीयक लॉगिंग सर्वर (Syslog सर्वर) लागू करें।
   - 8.1 जब प्राथमिक लॉग फाइलों को फायरवॉल में छेड़छाड़ की जाती है, तो Syslog सर्वर लॉग को संग्रहीत कर सकता है।
   - 8.2 Syslog सर्वर को सुरक्षित और सुदृढ़ किया जाना चाहिए।

182. बैकअप और अतिरेक

1. सुनिश्चित करें कि फायरवॉल में अतिरेक तंत्र है। इंटरनेट का सामना करने वाला फायरवॉल, उच्च उपलब्धता के लिए सक्रिय–सक्रिय मोड में लागू किया जाना चाहिए।
2. फायरवॉल रूल बेस का समय–समय पर बैकअप लिया जाना चाहिए।
   - 2.1 बैकअप की आवृत्ति रूल बेस में परिवर्तन की संख्या और रूल बेस की गंभीरता पर विचार करने के बाद निर्धारित की जानी चाहिए
   - 2.2 सिस्टम/फायरवॉल व्यवस्थापक को यह सुनिश्चित करना चाहिए कि बैकअप उपलब्ध हैं और रूल बेस तक पहुंच प्रतिबंधित है

2.2.1 सुनिश्चित करें कि रूल बेस का भौतिक मीडिया या केन्द्रीय फाइल सर्वर पर बैकअप लिया गया है।

2.2.2 यदि मीडिया पर संग्रहीत है, तो

2.2.2.1 इसमें मौजूद डाटा को एन्क्रिप्शन तंत्र द्वारा संरक्षित किया जाना चाहिए।

2.2.2.2 मीडिया तक भौतिक और तार्किक पहुंच को नियंत्रित किया जाना चाहिए और केवल सिस्टम/फायरवॉल व्यवस्थापक को प्रदान किया जाना चाहिए और जैसा कि सी.आई.एस.ओ. द्वारा अनुमोदित किया गया हो।

2.2.2.3 मीडिया में डाटा का निस्तारण करते समय मिटा दिया जाना चाहिए।

2.2.3 यदि केन्द्रीय फाइल सर्वर में संग्रहीत है, तो

2.2.3.1 फाइलों तक तार्किक पहुंच को नियंत्रित किया जाना चाहिए और केवल सी.आई.एस.ओ. और सिस्टम/फायरवॉल व्यवस्थापक को दिया जाना चाहिए।

2.2.3.2 सुनिश्चित करें कि सर्वर में रूल बेस रखा गया है और अनधिकृत पहुंच से संरक्षित किया जाना चाहिए

2.2.4 सुनिश्चित करें कि पुनर्प्राप्ति प्रक्रिया का पालन सुनिश्चित करने के लिए बैकअप एक परीक्षण सेटअप (यदि उपलब्ध हो) पर पुनर्प्राप्त किया गया है।

183. रिपोर्टिंग और प्रलेखन

1 सिस्टम/फायरवॉल व्यवस्थापक को फायरवॉल पर देखी गई किसी भी घटना के लिए सी.आई.एस.ओ. को रिपोर्ट करना चाहिए।

2 फायरवॉल रूल बेस परिवर्तन पर मासिक रिपोर्ट सी.आई.एस.ओ. को प्रदान की जानी चाहिए।

3 फायरवॉल लॉग समीक्षा की मासिक रिपोर्ट सी.आई.एस.ओ. को भेजी जाएगी।

4 रूल बेस परिवर्तन अनुरोध प्रपत्र का उपयोग रूल बेस परिवर्तनों को ट्रैक और स्वीकृत करने के लिए किया जाना चाहिए।

5 फायरवॉल इंस्टालेशन, कॉन्फिगरेशन, एडमिनिस्ट्रेशन आदि से संबंधित सभी अभिलेख केवल सी.आई.एस.ओ. और सिस्टम / फायरवॉल एडमिनिस्ट्रेटर को ही वितरित किए जाने चाहिए।

6 सभी अभिलेखों और दस्तावेजों को बंद अलमारियों में रखा जाना चाहिए या केन्द्रीय फाइल सर्वर में सुरक्षित फोल्डरों में संग्रहीत किया जाना चाहिए।

184. प्रयोज्यता

यह नीति यूकेएसडीसी के संचालन के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की जाती है।

185. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–26: सूचना सुरक्षा घटना प्रबंधन

186. प्रयोजन

इस नीति का उद्देश्य यह सुनिश्चित करना है कि सभी सुरक्षा उल्लंघनों या उल्लंघन के प्रयासों और सूचना प्रणाली में खोजी गई सभी सुरक्षा कमजोरियों की सूचना दी जानी चाहिए।

187. नीति कथन और उद्देश्य

घटना प्रबंधन प्रक्रिया को यह सुनिश्चित करना चाहिए कि सभी रिपोर्ट किए गए सुरक्षा उल्लंघनों या कमजोरियों का तुरंत जवाब दिया जाए और यूकेएसडीसी संगठन में पुनरावृत्ति को रोकने के लिए कार्यवाही की जाए।

188. नियंत्रण

(क) घटना की पहचानः

1 एक घटना एक स्पष्ट या निहित सूचना सुरक्षा नीति का उल्लंघन करने का कार्य है। निम्नलिखित क्रियाओं को घटनाओं के रूप में वर्गीकृत किया जा सकता है:

1.1 किसी सिस्टम या उसके डाटा तक अनधिकृत पहुँच प्राप्त करने का प्रयास; अधिकृत उपयोगकर्ताओं के रूप में स्वांग बनाना, धोखा देना।

1.2 अवांछित व्यवधान या सेवा से इनकार।

1.3 अधिकृत उपयोगकर्ताओं द्वारा डाटा के प्रसंस्करण या भंडारण के लिए सिस्टम का अनधिकृत उपयोग।

1.4 स्वामी की जानकारी, निर्देश या सहमति के बिना सिस्टम हार्डवेयर, फर्मवेयर या सॉफ़्टवेयर विशेषताओं और डाटा में परिवर्तन।

1.5 पथभ्रष्ट उपयोगकर्ता खातों का अस्तित्व।

2 ऐसी सूचना सुरक्षा घटनाओं की पहचान करने के लिए आईटी सिस्टम के सभी उपयोगकर्ताओं और प्रशासकों को जिम्मेदार होना चाहिए।

(ख) घटना की रिपोर्टिंग

1. यदि किसी उपयोगकर्ता को संदेह है कि कोई घटना हुई है, तो उसे तुरंत आईटी टीम को सूचित किया जाना चाहिए। टीम इसे सी.आई.एस.ओ. तक पहुंचाएगी।
2. नुकसान के कारण और सीमा का पता लगाने के लिए आईटी टीम को प्रारंभिक विश्लेषण करना चाहिए।
3. घटना की रिपोर्ट सी.आई.एस.ओ. को भेजी जानी चाहिए। रिपोर्ट में निम्नलिखित विवरण शामिल होने चाहिए।

3.1 घटना का विवरण,

3.2 संभावित कारण,

3.3 देखा गया नुकसान,

3.4 अनुपूरक प्रमाण,

3.5 उठाए गए उपचारात्मक कदम।

4. उपलब्ध आंकड़ों और घटना की गंभीरता के स्तर के आधार पर, सी.आई.एस.ओ. अधिकृत व्यक्ति को आवेदन समूहों और उपयोगकर्ता विभागों को घटना अलर्ट भेजने के लिए निर्देशित कर सकता है जो संभवतः इसी तरह की घटनाओं से प्रभावित हो सकते हैं।

(ग) घटना का सत्यापन

1. सी.आई.एस.ओ. को आईटी टीम से प्राप्त आंकड़ों के आधार पर घटनाओं की समीक्षा करनी चाहिए। यदि आवश्यक हो तो सी.आई.एस.ओ. को सिस्टम प्रशासकों से अधिक जानकारी लेनी चाहिए।
2. सी.आई.एस.ओ. को घटना को रिकॉर्ड करना चाहिए और ट्रैकिंग और भविष्य के संदर्भ के लिए घटना संख्या आवंटित करनी चाहिए।
3. एक बार घटना की वैधता सत्यापित हो जाने के बाद, सी.आई.एस.ओ. को समीक्षा और अनुमोदन के लिए डोमेन टीम से एक कार्य योजना प्राप्त करनी चाहिए।

(घ) घटना पुनर्प्राप्ति

1. पुनर्प्राप्ति योजना को क्रियान्वित करने के लिए आवश्यक सिस्टम कर्मियों से संपर्क किया जाना चाहिए।
2. यह सुनिश्चित करने के लिए कि सभी घटना संबंधी गतिविधियां बंद हो गई हैं, पुनर्प्राप्ति के बाद थोड़े समय के लिए अतिरिक्त निगरानी तंत्र तैनात किया जाना चाहिए।

(ङ) घटना की रोकथाम

1. घटना से सीख के आधार पर, सी.आई.एस.ओ. को सुरक्षा टीम को सुरक्षा नीतियों में आवश्यक परिवर्तन (यदि आवश्यक हो) करने के लिए निर्देशित करना चाहिए।
2. भविष्य के संदर्भों के लिए घटनाओं और पुनर्प्राप्ति चरणों का एक डाटाबेस बनाए रखा जाना चाहिए।

189. प्रयोज्यता

यह नीति यूकेएसडीसी के संचालन के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की जाती है।

190. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–27: सूचना संचालन, लेबलिंग और निस्तारण

191. प्रयोजन

सूचना धारक यूकेएसडीसी के प्रति इसके मूल्य और संवेदनशीलता के आधार पर सूचना के वर्गीकरण के लिए जिम्मेदार है।

192. नीति कथन और उद्देश्य

संवेदनशील सूचना डाटा वाले अभिलेखों और मीडिया को उचित रूप से लेबल, हैंडल और निस्तारण किया जाना चाहिए।

193. नियंत्रण

सूचना वर्गीकरण

सूचना धारक यूकेएसडीसी के प्रति इसके मूल्य और संवेदनशीलता के आधार पर सूचना के वर्गीकरण के लिए जिम्मेदार है।

सभी सूचना संपत्तियों को प्रमुखता से निम्नलिखित चिह्नों में से एक प्रदर्शित करना चाहिए:

(क) **गोपनीय** – सूचना, जिसका नुकसान, भ्रष्टाचार या अनधिकृत प्रकटीकरण यूकेएसडीसी के व्यावसायिक कार्यों को खराब करता है या जिसके परिणामस्वरूप व्यावसायिक, वित्तीय या विधिक हानि होती है। जैसे व्यक्तिगत डाटा, मजदूरी या वेतन कार्यक्रम, वित्तीय डाटा, अभिगम नियंत्रण डाटा, सूचना संसाधनों के सुरक्षा अभिलेख, रणनीतिक योजना, भर्ती योजना, बजट, ग्राहक डाटा और परियोजना से संबंधित डाटा।

(ख) **केवल आंतरिक उपयोग** – परिचालन डाटा जो यूकेएसडीसी की छवि या प्रतिष्ठा को गंभीर नुकसान नहीं पहुंचाएगा, या प्रतिस्पर्धात्मक लाभ की हानि, यदि खुलासा किया गया हो। यूकेएसडीसी में काम करने वाला कोई भी व्यक्ति इस सूचना तक पहुंच सकता है। उदाहरण: फोन सूचियां, गुणवत्ता नीतियां, प्रक्रियाएं और मानक।

(ग) **सार्वजनिक** – डाटा जो ऊपर उल्लिखित किसी भी वर्गीकरण में नहीं आता है। यह डाटा विशिष्ट प्रतिबंधों के बिना आम तौर पर उपलब्ध कराया जा सकता है। उदाहरण: प्रेस विज्ञप्तियां, मार्केटिंग ब्रोशर, पत्रिकाएं, न्यूजलेटर, नौकरी के विज्ञापन।

1. यूकेएसडीसी द्वारा निर्मित और अनुरक्षित सभी सूचना (जैसे डाटा, परियोजना–संबंधित डाटा, ग्राहक डाटा, विक्रेता जानकारी, वित्तीय, पेरोल, व्यक्तिगत जानकारी) को गोपनीय, आंतरिक और सार्वजनिक के रूप में वर्गीकृत किया जाना चाहिए।
2. यूकेएसडीसी की सभी सूचना परिसंपत्तियां, माध्यम की परवाह किए बिना (उदाहरण के लिए, कागज, टेप पर इलेक्ट्रॉनिक रूप, कार्ट्रिज, फ्लॉपी डिस्क, सीडी–रोम, सर्वर) और/या फॉर्म (जैसे, टेक्स्ट, ग्राफिक, वीडियो, आवाज) को वर्गीकृत किया जाना चाहिए।

3. सूचना वर्गीकरण दिशानिर्देश यूकेएसडीसी के सभी अधिकृत उपयोगकर्ताओं के लिए लागू और उपलब्ध होने चाहिए जो सूचना दस्तावेज और डाटा बनाते हैं।
4. यदि निर्दिष्ट नहीं किया गया है, तो डिफॉल्ट वर्गीकरण आंतरिक होना चाहिए।
5. अन्य संगठनों के अभिलेखों/मीडिया पर वर्गीकरण लेबलों की व्याख्या करने में सावधानी बरती जानी चाहिए, जिनकी समान नामित लेबल के लिए अलग–अलग परिभाषाएं हो सकती हैं।
6. सूचना संपत्तियों के समुच्चय को सबसे सुरक्षित वर्गीकरण स्तर के आधार पर वर्गीकृत किया जाना चाहिए; दूसरे शब्दों में, जब मिश्रित वर्गीकरण का डाटा एक ही फाइल में मौजूद हो, तो उसी फाइल का वर्गीकरण उच्चतम स्तर का वर्गीकरण होना चाहिए।
7. सूचना धारक इसके सूचना वर्गीकरण की आवधिक समीक्षा के लिए जिम्मेदार होगा।
8. अनावश्यक व्यावसायिक व्यय से बचने के लिए एक बार संवेदनशीलता बीत जाने के बाद सूचना धारक को सूचना डाटा के वर्गीकरण के स्तर को कम करना चाहिए। इन परिस्थितियों में सूचना धारक द्वारा परिवर्तन और समाप्ति तिथियां प्रदान की जानी चाहिए।
9. गोपनीय डाटा को सूचना धारक की पूर्व समीक्षा और अनुमोदन के बाद ही अवर्गीकृत किया जाना चाहिए। नए समूह को उपलब्ध कराने से पहले अवर्गीकृत गोपनीय डाटा को साफ किया जाना चाहिए।

(घ) सूचना लेबलिंग

i. भौतिक या इलेक्ट्रॉनिक स्वरूपों में सभी सूचना संपत्तियों को इसके वर्गीकरण के अनुसार लेबल किया जाना चाहिए।
ii. सार्वजनिक, गोपनीय, आंतरिक के रूप में परिभाषित सूचना डाटा को 'सार्वजनिक', 'गोपनीय' या 'केवल आंतरिक उपयोग' जैसे सुरक्षा लेबलिंग की आवश्यकता होती है।
iii. इलेक्ट्रॉनिक अभिलेखों के फुटर में सुरक्षा लेबल होने चाहिए.
iv. टाइप किए गए और मुद्रित अभिलेखों पर अभिलेख के प्रत्येक पृष्ठ के पाद लेख में लेबलिंग की मुहर होनी चाहिए।
v. इलेक्ट्रॉनिक मीडिया (सीडी, टेप, आदि) को मीडिया के लेबल पर इसके वर्गीकरण के साथ स्पष्ट रूप से चिह्नित किया जाना चाहिए।
vi. कवर पत्रों में पत्राचार की सामग्री में सुरक्षा लेबल प्रदर्शित होने चाहिए
vii. हार्डकॉपी अभिलेखों वाले फोल्डरों के आगे और पीछे सुरक्षा लेबल लगाए जाने चाहिए।
viii. यूकेएसडीसी के पास अपनी भौतिक प्रणालियों जैसे (लैपटॉप, डेस्कटॉप, सर्वर, नेटवर्क उपकरण, दूरसंचार उपकरण और अन्य उपकरण) के लिए परिसंपत्ति सूची और लेबलिंग प्रणाली होनी चाहिए।

(ङ) सूचना संग्रहण

1. सूचना धारक को यह सुनिश्चित करना चाहिए कि डाटा उनके सुरक्षा वर्गीकरण के आधार पर संग्रहीत किया जाता है।
2. सभी सूचना डाटा और स्टोरेज मीडिया को निर्माता के विनिर्देशों के अनुसार सुरक्षित और संरक्षित वातावरण में संग्रहित किया जाना चाहिए।

3. संवेदनशील सूचना को मोबाइल कंप्यूटिंग उपकरणों पर सुरक्षित रूप से संग्रहित किया जाना चाहिए।

(क) पावर–ऑन पासवर्ड,

(ख) पासवर्ड के साथ ऑटो लॉगऑफ या स्क्रीन सेवर, और

(ग) संग्रहीत डाटा या सी.आई.एस.ओ. द्वारा अनुमोदित अन्य स्वीकार्य सुरक्षा उपायों का एन्क्रिप्शन।

4. संवेदनशील सूचना डाटा वाले अभिलेखों और मीडिया को उपयोगकर्ता के कार्य क्षेत्र में, प्रिंटर या फैक्स मशीन के पास अप्राप्य नहीं रखा जाना चाहिए और केवल अधिकृत कर्मियों तक पहुंच के साथ उचित भौतिक सुरक्षा के साथ संग्रहीत किया जाना चाहिए।

5. सॉफ्टकॉपी में संवेदनशील सूचना को केवल अधिकृत कर्मियों तक पहुंच प्रदान करते हुए सुरक्षित रूप से संग्रहीत किया जाना चाहिए।

6. बैकअप मीडिया को पासवर्ड से सुरक्षित या बैकअप सॉफ्टवेयर का उपयोग करके एन्क्रिप्ट किया जाना चाहिए।

7. सूचना धारक को संवेदनशील सूचना का बैकअप लेना चाहिए। बैकअप के संबंध में निम्नलिखित विवरण सूचना धारक द्वारा प्रदान किया जाना चाहिए:

(क) किस सूचना का बैकअप लेने की आवश्यकता है,

(ख) सूचना का बैकअप कैसे लिया जाना चाहिए,

(ग) बैकअप की आवृत्ति,

(घ) बैकअप का प्रकार,

(ङ) मीडिया जिस पर सूचना का बैकअप होना चाहिए,

(च) वह समय जब सूचना का बैकअप लिया जाना चाहिए।

(च) सूचना हैंडलिंग

1. सूचना धारक यह सुनिश्चित करने के लिए जिम्मेदार है कि उसके नियंत्रण में सूचना को गोपनीयता, अखंडता और सूचना की उपलब्धता की रक्षा के लिए सूचना प्रबंधन और मीडिया निस्तारण नीति के अनुसार उचित रूप से वर्गीकृत और नियंत्रित किया जाता है।

2. सूचना धारक को डाटा तक पहुँचने के लिए अधिकृत उपयोगकर्ताओं या उपयोगकर्ता समूहों के लिए एक औपचारिक रिकॉर्ड की पहचान करनी चाहिए और उसे बनाए रखना चाहिए।

3. सुरक्षा प्रक्रियाओं, ऑपरेटिंग मैनुअल और ऑपरेटिंग रिकॉर्ड जैसी संवेदनशील सूचना को लॉक करने योग्य अलमारी में वर्गीकृत और सुरक्षित किया जाना चाहिए।

4. सूचना धारक को यह सुनिश्चित करना चाहिए कि सूचना डाटा का वितरण पूर्ण न्यूनतम और आवश्यकता के आधार पर रखा गया है।

5. महत्वपूर्ण सूचना और डाटा को सुरक्षित रूप से संभाला जाना चाहिए।

6. उपभोक्ताओं को कागज, डिस्क और अन्य प्रलेखन के लिए एक स्पष्ट डेस्क नीति अपनाने के लिए प्रोत्साहित किया जाना चाहिए ताकि व्यावसायिक कार्यावधि के बाहर अनधिकृत पहुंच, हानि या सूचना के नुकसान के जोखिम को कम किया जा सके।

7. सिस्टम प्रलेखन तक पहुंच केवल आवश्यकता के आधार पर होनी चाहिए और सूचना धारक द्वारा अधिकृत होनी चाहिए।

8. सुनिश्चित करें कि बाहरी मूल के अभिलेख सुरक्षित रूप से संग्रहीत और अधिकृत कर्मियों को ही वितरित किए जाते हैं (जैसे: प्रस्ताव, मूल्य सूची, प्रस्तुतियाँ आदि)
9. सूचना धारक को नियमित अंतराल में वितरण सूचियों और अधिकृत कर्मियों की सूचियों की समीक्षा करनी चाहिए।
10. सी.आई.एस.ओ. को समय–समय पर अनुपालन स्तर निर्धारित करने के लिए आंतरिक लेखापरीक्षा रिपोर्ट की समीक्षा करनी चाहिए।
11. गोपनीय सूचना को एक विभाग से दूसरे विभाग में या उत्पादन से संग्रह में स्थानांतरित करने से पहले सूचना धारक को अनुमोदन लेना चाहिए। उदाहरण: प्रोजेक्ट डाटा को विकास से संग्रह में ले जाना।
    i. नए सूचना धारक को यह सुनिश्चित करना चाहिए कि सूचना स्वामित्व का हस्तांतरण होने पर डाटा पिछले/प्रथम धारक के लिए उपलब्ध नहीं है।
    ii. यह प्रक्रिया डाटा के दोहराव से बचाती है।
    iii. पिछले धारक द्वारा गोपनीय डाटा का अनुरोध करने के मामले में, वर्तमान/नए सूचना धारक को इसे अनुमोदित करना होगा।

(छ) सूचना संचरण

सूचना धारक से पूर्व प्राधिकरण/अनुमोदन के बिना सूचना परिसर से बाहर नहीं भेजी जानी चाहिए।

लिफाफा डाक में भेजी गई अत्यधिक संवेदनशील सूचना को "गोपनीय" के रूप में चिह्नित किया जाना चाहिए और मुहरबंद किया जाना चाहिए।

सीलबंद लिफाफा प्रमाणित रिटर्न रसीद के साथ ट्रेस करने योग्य डिलीवरी विकल्प के साथ भेजा जाना चाहिए।

अधिकृत कुरियर एजेंसियों की सूची यूकेएसडीसी द्वारा अनुमोदित की जानी चाहिए और उन एजेंसियों की पहचान सत्यापित करने की प्रक्रिया लागू की जानी चाहिए।

ईमेल के माध्यम से संवेदनशील सूचना भेजने के लिए आधिकारिक ईमेल–आईडी का उपयोग किया जाना चाहिए।

यदि अत्यधिक संवेदनशील सूचना को ईमेल पर कई लोगों को भेजने की आवश्यकता है, तो इसे सूचना धारक द्वारा अनुमोदित किया जाना चाहिए।

असुरक्षित प्रथाओं के कारण संवेदनशील सूचना अनजाने में प्रकट हो सकती है। नीचे उल्लिखित परिदृश्यों में संवेदनशील सूचना की सुरक्षा के लिए सर्वोत्तम प्रथाओं का पालन किया जाना चाहिए:

अन्य कर्मचारियों की उपस्थिति में गोपनीय सूचना पर चर्चा करना, जिन्हें सूचना को "जानने की आवश्यकता नहीं" है:–

(क) सार्वजनिक स्थानों पर गोपनीय अभिलेख पढ़ना,
(ख) सार्वजनिक स्थानों पर गोपनीय सूचना पर चर्चा,

(ग) सार्वजनिक स्थानों पर लैपटॉप पर काम करना,

i. मोबाइल फोन पर गोपनीय सूचना पर चर्चा करना (पासवर्ड, क्रेडिट कार्ड नंबर आदि साझा करना)

(घ) आंसरिंग मशीन पर गोपनीय सूचना छोड़ना,

i. असत्यापित व्यक्तियों को फोन पर प्रश्नों का उत्तर देना (सोशल इंजीनियरिंग हमला)।

(ङ) विक्रेताओं / आपूर्तिकर्ताओं को सूचना प्रदान करना।

i. इंटरनेट पर सूचना प्रदान करना जैसे मेलिंग सूची, निजी फोरम, वेब साइट।

(च) एक ही मीडिया में संवेदनशील और गैर–संवेदनशील जानकारी संग्रहीत करना।

(ज) सूचना पुनरुत्पादन

निजी डाटा के पुनरुत्पादन की अनुमति नहीं दी जानी चाहिए। गोपनीय सामग्री का पुनरुत्पादन (जैसे सिस्टम प्रलेखन, सुरक्षा प्रक्रिया, ऑपरेटिंग मैनुअल, ऑपरेटिंग रिकॉर्ड इत्यादि) पूर्ण न्यूनतम आवश्यकता होगी और केवल सूचना धारक के अनुमोदन से ही किया जाना चाहिए। आंतरिक वर्गीकृत डाटा का पुनरुत्पादन सूचना धारक के विवेक पर छोड़ दिया गया है।

(झ) सूचना एवं मीडिया निस्तारण

1. सूचना धारक को यह सुनिश्चित करना चाहिए कि डाटा उसके जीवनकाल के बाद नष्ट हो जाए।
2. सूचना के निस्तारण को संवेदनशील या गोपनीय सूचना की निरंतर सुरक्षा सुनिश्चित करनी चाहिए।
3. गोपनीय या संवेदनशील सूचना रखने वाले सभी संग्रहीत मीडिया को रिकॉर्ड प्रतिधारण कार्यक्रम के अनुसार सुरक्षित रूप से नष्ट कर दिया जाना चाहिए। कॉपी करने, प्रिंट करने या फैक्स करने के दौरान उत्पन्न संवेदनशील सूचना की सभी बेकार प्रतियों को पेपर श्रेडर का उपयोग करके काटा जाना चाहिए।
4. यदि कर्मचारी संवेदनशील सूचना की प्रतियां बनाते समय कॉपी मशीन जाम या खराब हो जाती है, तो शामिल कर्मचारी को मशीन छोड़ने से पहले सूचना को पुनः प्राप्त करना चाहिए।
5. वॉयस और वीडियो रिकॉर्डिंग को उनके निस्तारण से पहले टेप से मिटा दिया जाना चाहिए।
6. स्टोरेज मीडिया जैसे हार्ड ड्राइव या हटाने योग्य मीडिया जैसे टेप ड्राइव, यूएसबी ड्राइव को स्वरूपित या मिटा दिया जाना चाहिए यदि मीडिया का पुनः उपयोग किया जाना है।
7. सभी डेस्कटॉप और लैपटॉप की हार्ड डिस्क ड्राइव को फिर से उपयोग करने या रखरखाव के लिए भेजने से पहले निम्न स्तर की फॉर्मेटिंग की जानी चाहिए।
8. फ्लॉपी डिस्क, हार्ड ड्राइव, ज़िप डिस्क आदि जैसे चुंबकीय मीडिया को त्यागने से पहले मिटा दिया जाना चाहिए।
9. फ्लॉपी, सीडी या टेप/ऑप्टिकल मीडिया जैसे एक्सपायर्ड या दूषित स्टोरेज मीडिया को इसके निस्तारण से पहले डिगॉस या मिटा दिया जाना चाहिए।
10. निस्तारण से पहले उपकरण से संवेदनशील डाटा और लाइसेंस प्राप्त सॉफ्टवेयर को पूरी तरह से सुरक्षित रूप से मिटा दें।
11. मीडिया को इसके निस्तारण से पहले भौतिक रूप से नष्ट कर दिया जाना चाहिए।

12. स्थायी मीडिया जैसे सीडीरॉम और फ्लॉपी डिस्क को खुरच कर विरूपित किया जाना चाहिए, आधे में तोड़ा जाना चाहिए, या त्यागने से पहले टुकड़े–टुकड़े कर दिया जाना चाहिए।
13. बैकअप मीडिया को डीगॉस करें और सुरक्षित निस्तारण प्रक्रिया के रूप में टेपों को काटें।
14. सभी मीडिया को हटाने/निपटान करने के लिए उचित प्राधिकरण की आवश्यकता होनी चाहिए।
15. सूचना धारक को मीडिया निस्तारण के लिए प्राधिकरण पर हस्ताक्षर करना चाहिए, निस्तारण हेतु मीडिया को चिह्नित करना चाहिए।
16. सूचना धारक को निस्तारण के लिए चिह्नित वस्तुओं के पिकअप का समय निर्धारित करना चाहिए या संबंधित विभाग से औपचारिक रूप से यूकेएसडीसी परिसर में स्थित निस्तारण स्थल पर वस्तुओं को स्थानांतरित करना चाहिए।
17. यूकेएसडीसी के परिसर में सभी प्रकार के सूचना मीडिया (उदाहरण के लिए, कागज, टेप पर इलेक्ट्रॉनिक रूप, कार्ट्रिज, फ्लॉपी डिस्क, सीडी–रोम, सर्वर) का निस्तारण किया जाना चाहिए।
18. इलेक्ट्रॉनिक मीडिया के किसी भी निस्तारण को पर्यावरणीय नियमों का पालन करना चाहिए।
19. निम्नलिखित सूची उन वस्तुओं की पहचान करती है जिन्हें सुरक्षित निस्तारण की आवश्यकता हो सकती है:
    (एक) कागजी अभिलेख,
    (दो) वॉइस या अन्य रिकॉर्डिंग,
    (तीन) आउटपुट रिपोर्ट,
    (चार) हटाने योग्य डिस्क,
    (पाँच) ऑप्टिकल स्टोरेज मीडिया (सभी रूप और सभी निर्माता सॉफ्टवेयर वितरण मीडिया सहित) सी.डी.
    (छः) सिस्टम प्रलेखन।
20. यदि निस्तारण आउटसोर्स किया जा रहा है, तो सामान्य निस्तारण व्यवस्था के लिए जिम्मेदार बाहरी ठेकेदारों के पास उचित सुरक्षा और प्रक्रिया जांच होनी चाहिए ताकि यह सुनिश्चित हो सके कि जानकारी सुरक्षित तरीके से निस्तारित की जा रही है।
21. आउटसोर्सिंग निस्तारण के लिए यूकेएसडीसी और बाहरी ठेकेदार के बीच गैर–प्रकटीकरण समझौते पर हस्ताक्षर किए जाने चाहिए।
22. बाहरी ठेकेदार से "सुरक्षित निस्तारण का प्रमाण पत्र" प्राप्त किया जाना चाहिए।
23. बाहरी ठेकेदार को उन कर्मियों की एक सूची प्रदान करनी चाहिए जिन्हें यूकेएसडीसी परिसर के भीतर कचरे के संग्रह के लिए सुरक्षित निस्तारण क्षेत्र तक पहुंच की आवश्यकता होगी।
24. यूकेएसडीसी परिसर के भीतर सुरक्षित निस्तारण क्षेत्र तक पहुंच के लिए संगठन को बाहरी ठेकेदार को विक्रेता पहचान पत्र प्रदान करना चाहिए।
25. यदि निस्तारण के लिए तीसरे पक्ष के ठेकेदारों द्वारा मैग्नेटिक मीडिया को ऑफ–साइट ले जाया जा रहा है, तो इन तीसरे पक्ष के ठेकेदारों को गोपनीयता समझौतों से बाध्य होना चाहिए।
26. संवेदनशील सूचना को हटाने और/या निस्तारण का रिकॉर्ड रखा जाना चाहिए।
27. ऑडिट ट्रेल को बनाए रखने के लिए गोपनीय और आंतरिक वस्तुओं का निस्तारण लॉग किया जाना चाहिए। गोपनीय लेबल वाली सूचना संपत्ति या अभिलेखों का निस्तारण सुरक्षित रूप से किया जाना चाहिए और संरक्षक द्वारा देखा जाना चाहिए।

28. प्राप्तकर्ताओं में से प्रत्येक को सूचित किया जाना चाहिए कि या तो आगे वितरण या अतिरिक्त प्रतिलिपि सूचना धारक की लिखित अनुमति प्राप्त करने के बाद ही हो सकती है।
29. यदि गोपनीय सूचना मुद्रित की जा रही है या शीघ्र ही मुद्रित की जाएगी, तो प्रिंटरों को अप्राप्य नहीं छोड़ा जाना चाहिए। प्रिंटर में उपस्थित होने वाले कार्मिकों को मुद्रित की जा रही सूचना की जांच करने के लिए अधिकृत होना चाहिए। यदि प्रिंटर के आस–पास का क्षेत्र भौतिक रूप से सुरक्षित है, तो अप्राप्य मुद्रण की अनुमति है, जैसे कि जो कर्मचारी सामग्री को देखने के लिए अधिकृत नहीं हैं, उन्हें प्रवेश करने की अनुमति नहीं है।

194. प्रयोज्यता

यह नीति यूकेएसडीसी के संचालन के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की जाती है।

195. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय 28: अनुश्रवण

196. प्रयोजन

इस नीति का प्रयोजन यह सुनिश्चित करना है कि सभी प्रणालियों और उपकरणों द्वारा उत्पन्न लॉग की निगरानी करने और दैनिक/साप्ताहिक आधार पर लॉग की समीक्षा करने के लिए एक कर्मचारी को नियुक्त किया जाए।

197. नीति कथन और उद्देश्य

सुरक्षा संबंधी किसी भी घटना के लिए अनुश्रवण तथा समीक्षा की गई गतिविधियों की स्थिति पर व्यक्ति को साप्ताहिक आधार पर सी.आई.एस.ओ. को रिपोर्ट करना चाहिए।

198. नियंत्रण

(क) अनुश्रवण टीम

1. सभी प्रणालियों और उपकरणों द्वारा उत्पन्न लॉग की निगरानी करने और साप्ताहिक आधार पर लॉग की समीक्षा करने के लिए कर्मियों को नियुक्त किया जाना चाहिए।
2. सुरक्षा संबंधी किसी भी घटना के लिए अनुश्रवण तथा समीक्षा की गई गतिविधियों की स्थिति पर व्यक्ति को साप्ताहिक आधार पर सी.आई.एस.ओ. को रिपोर्ट करना चाहिए।

(ख) अनुश्रवण

1. किसी भी सूचना सुरक्षा घटना को रिकॉर्ड करने के लिए लॉग मॉनिटरिंग सिस्टम होना चाहिए।
2. वास्तविक समय नेटवर्क–आधारित हमलों, प्रशासनिक गतिविधियों और अनधिकृत पहुंच की निगरानी के लिए आईडीएस स्थापित किया जाना चाहिए।
3. दोषों को लॉग किया जाना चाहिए, उनका विश्लेषण किया जाना चाहिए और उन पर उचित कार्यवाही की जानी चाहिए।
   3.1 सुनिश्चित करें कि उपयोगकर्ता दोषों/त्रुटियों की रिपोर्ट करने से अवगत है।
   3.2 यह सुनिश्चित करने के लिए सुधारात्मक और निवारक उपाय प्रदान करें कि दोष फिर से न हों।
4. लॉगिंग का स्तर सावधानी से निर्धारित किया जाना चाहिए क्योंकि यदि प्रतिदिन बड़ी मात्रा में लॉग उत्पन्न होते हैं तो सिस्टम का प्रदर्शन प्रभावित हो सकता है।
5. बाहरी लोगों द्वारा की जाने वाली निगरानी में गैर–प्रकटीकरण अनुबंध (एन.डी.ए.) और सेवा स्तर के समझौते (एस.एल.ए.) शामिल होने चाहिए।
   5.1 एसएलए को समीक्षा गतिविधियों के अनुश्रवण और लॉगिंग हेतु रिपोर्टिंग तंत्र का उल्लेख करना चाहिए।

(ग) ऑडिट लॉगिंग

1. ऑडिट लॉग सभी महत्वपूर्ण सर्वर, एप्लिकेशन और डाटाबेस, नेटवर्क और सुरक्षा उपकरणों के लिए रिकॉर्ड किए जाने चाहिए।
2. महत्वपूर्ण फाइलों के लिए एक्सेस लॉग बनाए रखे जाएंगे।
3. ऑडिट लॉग जिन्हें पहचानने और समीक्षा करने की आवश्यकता है वे हैं:

3.1 सर्वर लॉग:

- 3.1.1 उपयोगकर्ता आई.डी.,
- 3.1.2 इवेंट लॉग दिनांक, समय, लॉग–इन, लॉग–ऑफ,
- 3.1.3 सुरक्षा लॉग,
- 3.1.4 प्रमाणीकरण विफलता,
- 3.1.5 खाता बनाया/हटाया/अक्षम किया गया,
- 3.1.6 विशेषाधिकार प्राप्त खातों के लिए पासवर्ड परिवर्तन,
- 3.1.7 सुरक्षा विन्यास सेटिंग्स में परिवर्तन,
- 3.1.8 सेवा का प्रारंभ और विराम,
- 3.1.9 सिस्टम त्रुटियाँ या विफलताएँ,
- 3.1.10 विशेषाधिकारों का उपयोग,

3.2 एप्लिकेशन लॉग

- 3.2.1 उपयोगकर्ता की पहुंच; लॉग इन लॉग ऑफ,
- 3.2.2 विशेषाधिकारों का उपयोग,
- 3.2.3 एप्लिकेशन में परिवर्तन,
- 3.2.4 पासवर्ड परिवर्तन,
- 3.2.5 एप्लिकेशन त्रुटियां/विफलताएं,
- 3.2.6 एप्लिकेशन सेवा प्रारंभ/विराम,

3.3 नेटवर्क और सुरक्षा उपकरण लॉग,

- 3.3.1 लॉगिन और लॉग–ऑफ प्रयासों की संख्या,
- 3.3.2 कॉन्फिगरेशन परिवर्तन,
- 3.3.3 कंसोल अलर्ट।

4. सभी व्यवस्थापक गतिविधियों को नियमित आधार पर लॉग इन और समीक्षा की जानी चाहिए।
5. सभी सर्वर और नेटवर्क डिवाइस समय को एक सहमत सटीक समय स्रोत के साथ सिंक्रनाइज़ किया जाना चाहिए।

(घ) लॉग सूचना का संरक्षण

1. अनधिकृत उपयोगकर्ताओं द्वारा हटाए जाने से बचने के लिए सिस्टम को केन्द्रीय लॉग सर्वर पर लॉग पुश करने के लिए कॉन्फिगर किया जा सकता है।
2. लॉग तक पहुंच केवल आवश्यक कर्मियों तक ही सीमित होनी चाहिए।

3. किसी भी उपयोगकर्ता को लॉग को संशोधित करने की अनुमति नहीं दी जानी चाहिए। केवल सिस्टम लॉग फाइलों में लिखने में सक्षम होना चाहिए।

(ङ) **बैकअप**

1. कानूनी आवश्यकताओं का पालन करने और सुरक्षा घटना के दौरान भविष्य के संदर्भों के लिए लॉग का नियमित आधार पर बैकअप लिया जाएगा।
2. यूकेएसडीसी की रिकॉर्ड प्रतिधारण प्रक्रिया के अनुसार लॉग को बनाए रखें।

(च) **प्रलेखन**

1. अनुश्रवण कर्मियों को निगरानी प्रक्रिया, रिकॉर्ड, लॉग कॉन्फिगरेशन अभिलेखों आदि से संबंधित अद्यतन अभिलेखों को अनुरक्षित रखना चाहिए।
2. इन दस्तावेजों और अभिलेखों की पहुंच और वितरण को नियंत्रित किया जाना चाहिए।

(छ) **घटना की रिपोर्टिंग**

1. सिस्टम एडमिनिस्ट्रेटर को सिस्टम की अनुश्रवण गतिविधियों पर सी.आई.एस.ओ. को रिपोर्ट करना चाहिए।
2. किसी भी घटना को तुरंत घटना प्रबंधन प्रक्रिया और/या समस्या प्रबंधन प्रक्रिया शुरू करनी चाहिए।

199. प्रयोज्यता

यह नीति यूकेएसडीसी के संचालन के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की जाती है।

200. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय 29: नेटवर्क सुरक्षा

201. प्रयोजन

इस नीति का उद्देश्य यह सुनिश्चित करना है कि यूकेएसडीसी संगठन के नेटवर्क तक सभी पहुंच सुरक्षित है यह सुनिश्चित करने के लिए प्रक्रियाओं को परिभाषित, विकसित और उपायों को लागू किया जाता है।

202. नीति कथन और उद्देश्य

इस नीति का उद्देश्य यूकेएसडीसी नेटवर्क में सभी प्रकार की पहुंच के सुरक्षा स्तर को बनाए रखना है।

203. नियंत्रण

(क) नेटवर्क टीम

1. यूकेएसडीसी नेटवर्क के प्रबंधन के लिए एक टीम को परिभाषित किया जाना चाहिए।
2. नेटवर्क उपलब्धता और प्रदर्शन पर सी.आई.एस.ओ. को मासिक रिपोर्ट भेजी जानी चाहिए।
3. नेटवर्क में किसी भी गंभीर/बड़ी घटना की सूचना सी.आई.एस.ओ. को दी जानी चाहिए।
4. नेटवर्क में किसी भी नई भेद्यता का पता लगाया जाना चाहिए और उस पर उचित कार्यवाही की जानी चाहिए।

(ख) इंटरनेट एक्सेस

1. सभी उपयोगकर्ताओं के लिए इंटरनेट का उपयोग एक केन्द्रीय गेटवे द्वारा नियंत्रित किया जाना चाहिए। इंटरनेट का उपयोग प्रॉक्सी सर्वर के माध्यम से हो सकता है।
2. सभी उपयोगकर्ताओं को इंटरनेट एक्सेस के लिए अपने विभाग प्रमुख से अनुमोदन प्राप्त करना चाहिए।
3. पहुंच की अनुमति देने से पहले सभी उपयोगकर्ताओं को प्रमाणित किया जाना चाहिए। इंटरनेट एक्सेस विशेषाधिकार रखने वाले सभी उपयोगकर्ताओं के पास एक अद्वितीय उपयोगकर्ता–आई.डी. और पासवर्ड होना चाहिए।
4. इंटरनेट कनेक्शन एक फायरवॉल द्वारा सुरक्षित किया जाना चाहिए। फायरवॉल को इंटरनेट प्रॉक्सी में किसी भी इनबाउंड एक्सेस को रोकना चाहिए।
5. सभी इंटरनेट ट्रैफिक को स्कैन करने के लिए गेटवे एंटी–वायरस स्थापित किया जाना चाहिए। सभी http ट्रैफिक और फाइल डाउनलोड को वायरस के लिए स्कैन किया जाना चाहिए।
6. इंटरनेट का प्रयोग केवल व्यावसायिक उद्देश्यों के लिए ही किया जाना चाहिए। यह सुनिश्चित करने के लिए इंटरनेट का उपयोग नियंत्रित किया जाना चाहिए कि केवल व्यवसाय से संबंधित साइटें ही पहुंच योग्य हैं। अनुमत वेब साइटों के लिए स्वीकार्य उपयोग नीति देखें।
7. आवश्यक वेबसाइटों को फिल्टर करने के कार्य को स्वचालित करने के लिए URL फिल्टरिंग सॉफ्टवेयर का उपयोग किया जाना चाहिए।

8. एक्सेस कंट्रोल डिवाइस को आवश्यक आई.पी.–एड्रेस और पोर्ट तक पहुंच को प्रतिबंधित करना चाहिए।
9. नेटवर्क ट्रैफिक (नेटवर्क इंट्रूज़न प्रिवेंशन सिस्टम्स (एन.आई.पी.एस) और होस्ट इंट्रूज़न प्रिवेंशन सिस्टम्स (एच.आई.पी.एस)) पर नज़र रखने के लिए आई.डी.एस. स्थापित किया जाना चाहिए।

(ग) नेटवर्क एक्सेस

1. नेटवर्क तक उपयोगकर्ता की पहुंच को सक्रिय निर्देशिका पर प्रमाणित किया जाना चाहिए। नेटवर्क तक पहुँचने वाले सभी उपयोगकर्ताओं के पास विशिष्ट उपयोगकर्ता आई.डी. होनी चाहिए।
2. जब उपयोगकर्ता संगठन छोड़ता है तो उपयोगकर्ता के लिए सभी नेटवर्क एक्सेस को हटा दिया जाना चाहिए।
3. संबंधित विभाग प्रमुख या उसके द्वारा अधिकृत व्यक्ति से अधिकारों और विशेषाधिकारों के लिए आवश्यक अनुमोदन के बाद ही नेटवर्क एक्सेस की अनुमति दी जानी चाहिए।
4. नेटवर्क और सुरक्षा उपकरणों तक प्रशासनिक पहुंच को नियंत्रित किया जाना चाहिए।
5. नेटवर्क और सुरक्षा उपकरणों तक भौतिक पहुंच को नियंत्रित किया जाना चाहिए।
6. दो यूकेएसडीसी नेटवर्क के बीच पहुंच को व्यावसायिक आवश्यकताओं के आधार पर प्रतिबंधित किया जाना चाहिए।
7. वायरस और वर्म को फैलने से और अनधिकृत पहुंच रोकने के लिए स्विच पर नेटवर्क एक्सेस कंट्रोल लिस्ट लागू करें
8. सुनिश्चित करें कि अवांछित ट्रैफिक को रोकने के लिए फायरवॉल पर केवल आवश्यक सेवाएँ ही सक्षम हैं।
9. महत्वपूर्ण बहु–उपयोगकर्ता एप्लिकेशन सर्वर को फायरवॉल द्वारा उपयोगकर्ता खंडों से अलग किया जाना चाहिए।
10. उत्पादन वातावरण को परीक्षण वातावरण से अलग करें।
11. विशिष्ट स्थानों या अन्य प्रणालियों से कनेक्शन को प्रमाणित करने के लिए सिस्टम को नेटवर्क में आसानी से पहचाना जा सकता है।
12. यूकेएसडीसी के सुरक्षा प्रबंधन से बाहर के बाहरी नेटवर्क से जुड़ने से पहले आईटी टीम को सी.आई.एस. ओ. से पूर्वानुमति लेनी चाहिए। इसमें ग्राहकों, आईटी सेवा प्रदाताओं और भागीदारों के कनेक्शन शामिल होने चाहिए। सी.आई.एस.ओ. को कनेक्शन से जुड़े जोखिमों पर विचार करना चाहिए और यह सुनिश्चित करना चाहिए कि जोखिमों को कम करने के लिए आवश्यक कदम उठाए जाएं।
13. नेटवर्क तक दूरस्थ पहुंच फायरवॉल पर समाप्त होनी चाहिए।
    - 13.1 फायरवॉल को उपयोगकर्ताओं को प्रमाणित करना चाहिए और फिर नेटवर्क में प्रवेश प्रदान करना चाहिए।
    - 13.2 सभी दूरस्थ उपयोगकर्ता गतिविधियों को लॉग किया जाना चाहिए।
14. रिमोट नेटवर्क को यूकेएसडीसी नेटवर्क को एक एन्क्रिप्टेड चैनल के माध्यम से एक्सेस करना चाहिए।
15. सूचना के आदान–प्रदान के दौरान रिमोट नेटवर्क द्वारा एक्सेस किए गए सभी डाटा को एन्क्रिप्ट किया जाना चाहिए।

16. ICMP अनुरोधों का जवाब देने से फायरवॉल पर एक्सेस कंट्रोल सूचियों को कॉन्फिगर किया जाना चाहिए।
17. सिस्टम के बीच रूटिंग व्यावसायिक अनुप्रयोगों और इन अनुप्रयोगों तक पहुँचने वाले उपयोगकर्ताओं की आवश्यकताओं के अनुसार होनी चाहिए।

(घ) बैकअप और अतिरेक

1. बैकअप नीति के अनुसार डिवाइस कॉन्फिगरेशन का समय–समय पर बैकअप लिया जाना चाहिए।
2. महत्वपूर्ण नेटवर्क लिंक के लिए पर्याप्त अतिरेक प्रदान किया जाना चाहिए। अतिरेक का स्तर लिंक का उपयोग करने वाले अनुप्रयोगों की महत्वपूर्णता पर निर्भर होना चाहिए। इंटरनेट कनेक्शन सहित महत्वपूर्ण लिंक के लिए, स्वचालित विफलता के साथ कॉन्फिगर किया गया एक अनावश्यक लिंक होना चाहिए ताकि यह सुनिश्चित हो सके कि व्यवसाय में न्यूनतम व्यवधान हो।
3. अनावश्यक लिंक में प्राथमिक लिंक के समान सुरक्षा स्तर होना चाहिए।
4. यदि प्राथमिक लिंक एन्क्रिप्शन और फायरवॉल सुरक्षा प्रदान करता है, तो द्वितीयक लिंक में भी समान सुरक्षा स्तर होना चाहिए
5. सभी महत्वपूर्ण उपकरणों में पर्याप्त अतिरेक बनाया जाना चाहिए:
   - 5.1 नेटवर्क डिवाइस जैसे कोर स्विच आदि।
   - 5.2 सुरक्षा उपकरण जैसे फायरवॉल आदि।
   - 5.3 क्रिटिकल यूकेएसडीसी एप्लिकेशन सर्वर और डाटाबेस सर्वर आदि।
   - 5.4 एक्टिव डायरेक्ट्री डोमेन, प्रॉक्सी आदि जैसे इंफ्रास्ट्रक्चर एप्लीकेशन।

(ङ) क्लॉक सिंक्रोनाइज़ेशन

यूकेएसडीसी को यह सुनिश्चित करना चाहिए कि घड़ी के समय को सभी नेटवर्क उपकरणों, सुरक्षा उपकरणों, डेस्कटॉप और सर्वरों के साथ सिंक्रनाइज़ किया जाना चाहिए।

(च) प्रलेखन

1. यूकेएसडीसी के फायरवॉल/नेटवर्क/सिस्टम एडमिनिस्ट्रेटर को निम्नलिखित विवरणों के लिए विस्तृत अभिलेख बनाए रखने चाहिए:
   - 1.1 वर्तमान और अद्यतन नेटवर्क संरचना आरेख,
   - 1.2 स्विच/राउटर/लिंक गति सहित नेटवर्क कनेक्टिविटी,
   - 1.3 फायरवॉल सेगमेंट के साथ,
   - 1.4 एप्लिकेशन सर्वर विवरण,
   - 1.5 आई.पी. पते विवरण,
   - 1.6 एक्सेस सूची / फायरवॉल रूल बेस विवरण,
   - 1.7 स्वीकृत सॉफ्टवेयर सूची जिसका यूकेएसडीसी में उपयोग किया जा सकता है।

(छ) परिवर्तन नियंत्रण

1. सुरक्षा स्तर को बनाए रखने के लिए नेटवर्क में सभी परिवर्तन उचित प्राधिकरण के बाद किए जाने चाहिए।
   - 1.1 डोमेन टीम को परिवर्तन प्रबंधन समिति (सीएमसी) को अनुरोध देना चाहिए।
   - 1.2 नेटवर्क आर्किटेक्चर में परिवर्तन, परिवर्तन प्रबंधन प्रक्रिया के अधीन होना चाहिए।
   - 1.3 अभिगम नियंत्रण सूचियों में सभी परिवर्तनों को परिवर्तन प्रबंधन प्रक्रिया का पालन करना चाहिए। किसी भी बदलाव से पहले सी.एम.सी. की मंजूरी लेनी होगी।
   - 1.4 परिवर्तन प्रबंधन समिति, सुरक्षा निहितार्थ और आवश्यकता के आधार पर अनुरोध को स्वीकृत, संशोधित या अस्वीकार करेगी।
   - 1.5 परिवर्तन प्रबंधन समिति, नेटवर्क परिवर्तन को सत्यापित करने के लिए एक सत्यापनकर्ता को अधिकृत करेगी।
   - 1.6 सत्यापनकर्ता को परिवर्तन प्रबंधन समिति को एक रिपोर्ट देनी चाहिए।
2. परिनियोजन से पहले अभिगम नियंत्रण सूचियों में सभी परिवर्तनों का परीक्षण किया जाना चाहिए।
   - 2.1 मूल योजना से किसी भी विचलन को भी प्रलेखित किया जाना चाहिए।
   - 2.2 परीक्षण डाटा को अनधिकृत पहुंच से पर्याप्त रूप से संरक्षित किया जाना चाहिए।
3. नेटवर्क में किसी भी बदलाव की योजना व्यापार और सिस्टम की आवश्यकताओं और संभावित बाधाओं से बचने के लिए यूकेएसडीसी की सूचना प्रसंस्करण क्षमताओं में वर्तमान और अनुमानित रुझानों के आधार पर सावधानीपूर्वक बनाई जाएगी।
4. नए नेटवर्क सिस्टम या उन्नयन की स्वीकृति के लिए आवश्यकताओं और मानदंडों को परिभाषित, सहमत, प्रलेखित और परीक्षण किया जाना चाहिए।

(ज) विक्रेता समर्थन

आवश्यक अनुबंध (सेवा स्तर अनुबंध और गैर–प्रकटीकरण अनुबंध) को विक्रेता के साथ उनके समर्थन और दस्तावेज के लिए परिभाषित किया जाना चाहिए।

204. प्रयोज्यता

यह नीति यूकेएसडीसी के संचालन के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें यूकेएसडीसी नेटवर्क तक पहुंच प्रदान की जाती है।

205. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय 30: ऑपरेटिंग सिस्टम सुरक्षा

206. प्रयोजन

इस नीति का उद्देश्य यह सुनिश्चित करना है कि यूकेएसडीसी संगठन के आईटी सिस्टम से जुड़े जोखिमों को ऑपरेटिंग सिस्टम (ओ.एस.) एक्सेस को सुरक्षित करके स्वीकार्य स्तर तक प्रबंधित किया जाता है।

207. नीति कथन और उद्देश्य

ऑपरेटिंग सिस्टम के सबसे सुरक्षित कार्यान्वयन को संस्थापन के समय पर चुना जाना चाहिए और ऑपरेटिंग सिस्टम तक उपयोगकर्ता की पहुंच को प्रतिबंधित और मॉनिटर किया जाना चाहिए। विक्रेता द्वारा जारी किए गए सुरक्षा पैचों के सापेक्ष ऑपरेटिंग सिस्टम को चालू रखा जाना चाहिए। यह नीति यूकेएसडीसी की सभी आईटी प्रणालियों पर लागू होती है।

208. नियंत्रण

(क) उपयोगकर्ता प्रमाणीकरण

1. पहुँच प्रदान करने से पहले सभी ओएस उपयोगकर्ताओं को प्रमाणित किया जाना चाहिए।
2. सभी ओएस उपयोगकर्ताओं के पास एक अनन्य उपयोगकर्ता–आईडी होनी चाहिए।

(ख) अकाउंट नीति

1. ओएस को न्यूनतम पासवर्ड लंबाई लागू करनी चाहिए।
2. ओएस को पासवर्ड की समाप्ति को लागू करना चाहिए।
3. ओएस को पासवर्ड हिस्ट्री लागू करना चाहिए।
4. ओएस को खाता लॉकआउट सुविधा लागू करनी चाहिए।
5. गैर–आवश्यक उपयोगकर्ता खातों को हटा दिया जाना चाहिए।
6. अस्थायी उपयोगकर्ता खातों को उपयोग के तुरंत बाद हटा दिया जाना चाहिए।

(ग) नए उपयोगकर्ता प्रावधान

1. सभी ओ.एस. उपयोगकर्ता केवल विभाग प्रमुख/उसके द्वारा अधिकृत व्यक्ति से अनुमोदन के बाद ही बनाए जाने चाहिए।
2. उपयोगकर्ता अधिकारों को कम से कम विशेषाधिकार के सिद्धांत के आधार पर आवंटित किया जाना चाहिए।

(घ) उपयोगकर्ता क्रेडेंशियल्स की सुरक्षा

1. उपयोगकर्ता–आईडी और पासवर्ड को सुरक्षित तरीके से संग्रहीत करने के लिए ओएस को कॉन्फ़िगर किया जाना चाहिए।
2. नेटवर्क पर सुरक्षित तरीके से यूजर–आईडी और पासवर्ड भेजने के लिए ओएस को कॉन्फ़िगर किया जाना चाहिए।

(ङ) **लॉगिंग**

सभी महत्वपूर्ण गतिविधियों को ट्रैक करने के लिए ओएस में लॉगिंग सक्षम होनी चाहिए।

(च) **पैच अद्यतन**

ऑपरेटिंग सिस्टम को नवीनतम सुरक्षा पैच और हॉट–फिक्स के साथ अद्यतन किया जाना चाहिए।

(छ) **गैर–आवश्यक सेवाएं**

सभी एप्लिकेशन और ओएस सेवाएं जो सिस्टम के कामकाज के लिए आवश्यक नहीं हैं, उन्हें अक्षम कर दिया जाना चाहिए।

(ज) **लॉगिन बैनर**

ओ.एस. में एक प्रारंभिक लॉगिन संदेश कॉन्फ़िगर किया जाना चाहिए जिसमें कहा गया हो कि सिस्टम का उपयोग केवल अधिकृत गतिविधियों के लिए किया जाना चाहिए।

"**********WARNING**********
UNAUTHORIZED ACCESS PROHIBITED ----- NOTICE TO ALL USERS
****

"This system is the property of the Government of Uttarakhand. Access to this system is provided only to the authorized personnel and used for official purpose only. It is strictly forbidden to modify, destroy, delete or alter, steal, damage, record, share, unauthorized access, transmit data or program without a written consent of authorized person. Attempting to penetrate or access a system without authorization are punishable under the Government of Uttarakhand and IT Act Rules.
**********".

209. एंटी वायरस

1. वायरस संक्रमण के जोखिम वाले सभी सिस्टमों पर एंटी–वायरस सॉफ़्टवेयर स्थापित किया जाना चाहिए।
2. एंटी–वायरस सॉफ़्टवेयर को नवीनतम हस्ताक्षर पैटर्न के साथ अद्यतन किया जाना चाहिए।

210. समय समन्वयन:

सेंट्रल सर्वर से टाइम सिंक्रोनाइज़ करने के लिए सभी सिस्टम्स को कॉन्फ़िगर किया जाना चाहिए।

211. नामकरण की परंपरा

आसान पहचान सुनिश्चित करने और नाम के टकराव को रोकने के लिए ओएस स्तर पर होस्ट नाम निर्दिष्ट करते समय मानक नामकरण परंपराओं का उपयोग किया जाना चाहिए।

212. अनुश्रवण

1. सभी प्रकार के उपयोगकर्ता पहुँच अधिकारों की नियमित समीक्षा समय–समय पर की जानी चाहिए।
2. सुरक्षा और इष्टतम उपयोग सुनिश्चित करने के लिए महत्वपूर्ण ओएस मापदंडों की समय–समय पर निगरानी की जानी चाहिए।

213. परिवर्तन प्रबंधन

परिवर्तन प्रबंधन नीति के अनुपालन में ओएस के संबंध में परिवर्तन किया जाना चाहिए।

214. बैकअप और अतिरेक

सिस्टम एडमिनिस्ट्रेटर बैकअप और पुनर्प्राप्ति के लिए जिम्मेदार होता है। समय–समय पर पुनर्प्राप्ति की जांच कराते रहना चाहिए।

215. प्रलेखन

सिस्टम व्यवस्थापक को उचित सिस्टम कार्यक्षमता सुनिश्चित करने के लिए कॉन्फिगरेशन चरणों का प्रलेखन करना चाहिए।

216. प्रयोज्यता

यह नीति एस.डी.सी. के संचालन के साथ–साथ उन व्यक्तियों पर भी लागू होती है जिन्हें एस.डी.सी. नेटवर्क तक पहुंच प्रदान की जाती है।

217. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–31: स्वीकार्य उपयोग

218. प्रयोजन

इस अभिलेख का प्रयोजन, स्वीकार्य उपयोग नीति, आवश्यकताओं को बताना है और सभी कर्मचारियों के स्वीकार्य व्यवहार के लिए दिशानिर्देश निर्धारित करना है क्योंकि यह यूकेएसडीसी डाटा सेंटर संसाधनों से संबंधित है। इस नीति का पालन, जब लागू किया जाता है और ठीक से पालन किया जाता है, तो यूकेएसडीसी डाटा सेंटर सिस्टम, समाधान, संपत्ति, उपकरण और सूचना की गोपनीयता, उपलब्धता और अखंडता (सी.आई.ए) सुनिश्चित होनी चाहिए।

219. नीति वक्तव्य और उद्देश्य

यह नीति उत्तराखंड राज्य डाटा सेंटर (यूकेएसडीसी) के सभी हितधारकों से संबंधित है, जिन्हें यूकेएसडीसी के संसाधनों और परिसंपत्तियों तक किसी भी समय के लिए पहुंच प्रदान की जाती है।

220. नियंत्रण

(क) यूकेएसडीसी संसाधनों के व्यक्तिगत उपयोग की अनुमति नहीं है। कर्मचारियों को आवंटित सभी संसाधन यूकेएसडीसी के हैं और इनका उपयोग केवल व्यावसायिक उद्देश्यों के लिए किया जाना चाहिए।

(ख) सुरक्षा एक व्यक्तिगत जिम्मेदारी है और इसे बनाए रखना एक पेशेवर कर्तव्य है जो हर कर्मचारी के कंधों पर, पूरे दिन और हर दिन रहता है। यूकेएसडीसी के किसी भी कर्मचारी, ठेकेदार या इंटर्न को इस व्यक्तिगत जिम्मेदारी से छूट नहीं है। व्यक्तियों को सामान्य सुरक्षा दिशानिर्देशों को समझने और उनका पालन करने की आवश्यकता है, लेकिन उन नीतियों पर विशेष ध्यान देने की आवश्यकता है जो उनके कार्य क्षेत्र से संबंधित हैं। जब कर्मचारी यूकेएसडीसी के संसाधनों और परिसंपत्तियों का उपयोग कर रहे हों, तो उन्हें अपने उपयोग के सुरक्षा पहलू को ध्यान में रखना होगा। यूकेएसडीसी संसाधनों और परिसंपत्तियों की सुरक्षा बनाए रखना इसके उचित उपयोग और उपयोग का हिस्सा है, और इसका पालन करने में विफलता के परिणामस्वरूप कर्मचारी को ऐसी विफलता के व्यक्तिगत परिणामों का सामना करना पड़ सकता है।

(ग) डाटा सेंटर के प्रभारी द्वारा नियमित रूप से जारी किए गए निर्देशों और दिशानिर्देशों का पालन करना कर्मचारी की व्यक्तिगत जिम्मेदारी है और संसाधनों और परिसंपत्तियों के स्वीकार्य उपयोग का हिस्सा है। इन नियमित रूप से अद्यतन दिशा–निर्देशों के बारे में अनभिज्ञता (ज्ञान/अज्ञानता की कमी) की दलील देना एक वैध या स्वीकार्य बहाना नहीं है।

(घ) यूकेएसडीसी संसाधनों पर संग्रहीत, संसाधित, प्रेषित, या संभाली गई सभी जानकारी उत्तराखंड राज्य डाटा सेंटर की एक संपत्ति है। नतीजतन, उत्तराखंड राज्य डाटा सेंटर को ऐसी संपत्ति और संसाधनों और उनके माध्यम से यात्रा करने वाली सूचना की निगरानी और ऑडिट करने का अधिकार है।

(ङ) उत्तराखंड राज्य डाटा सेंटर अपने व्यवसाय की महत्वपूर्ण प्रकृति के कारण अपनी सूचना की गोपनीयता को अपनी सर्वोच्च प्राथमिकताओं में से एक मानता है। उत्तराखंड राज्य डाटा सेंटर से संबंधित सूचना की प्रतिलिपि, पुनरुत्पादन, भंडारण या संचारण, उत्तराखंड राज्य डाटा सेंटर में उचित अधिकारियों से उचित अनुमोदन के बिना स्वीकार नहीं किया जा सकता क्योंकि यह सूचना गोपनीयता का गंभीर उल्लंघन है।

(च) पासवर्ड, पासवर्ड संकेत, सुरक्षा कोड और सुरक्षित शब्दों को बनाए रखना और अनुरक्षण प्रत्येक कर्मचारी की व्यक्तिगत जिम्मेदारी है। व्यक्तिगत संबंधों या अधिकार की स्थिति की निकटता की परवाह किए बिना ऐसी सूचना को अन्य कर्मचारियों के साथ साझा नही किया जा सकता है। पासवर्ड नीति के अनुसार नियमित रूप से पासवर्ड बदलना कर्मचारी की भी जिम्मेदारी है क्योंकि ऐसा करने में विफलता के परिणामस्वरूप उत्तराखंड राज्य डाटा सेंटर के संसाधनों और संपत्तियों को नुकसान हो सकता है।

(छ) जीयूआई के साथ सभी डेस्कटॉप कंप्यूटर, लैपटॉप और अन्य संवेदनशील उपकरणों में पासवर्ड से सुरक्षित स्क्रीनसेवर (या उपकरण की प्रकृति के आधार पर समकक्ष सुविधा) होना चाहिए। पासवर्ड सुरक्षा को 3 मिनट से अधिक निष्क्रिय रहने की अवधि के बाद सेल्फ–लॉन्च पर सेट किया जाना चाहिए।

(ज) डेस्कटॉप, लैपटॉप और स्टोरेज मीडिया पर संग्रहीत सभी संवेदनशील सूचना पासवर्ड से सुरक्षित होनी चाहिए। उत्तराखंड राज्य डाटा सेंटर के संसाधनों को पासवर्ड–संरक्षित संवेदनशील डाटा में विफल करके सुरक्षा के संभावित उल्लंघन के अधीन करना स्वीकार्य उपयोग का उल्लंघन है।

(झ) सभी मशीनों को नवीनतम एंटी–वायरस सॉफ्टवेयर चलाना चाहिए। किसी भी कर्मचारी को वायरस डिटेक्शन इंजन को अक्षम या निष्क्रिय करने की अनुमति नहीं है। उत्तराखंड स्टेट डाटा सेंटर में केवल आधिकारिक तौर पर स्वीकृत एंटी–वायरस समाधान ही इसकी मशीनों पर चल सकता है। अन्य एंटी–वायरस समाधानों के लिए कर्मचारी की व्यक्तिगत और अलग–अलग प्राथमिकताएं यह चुनने का कारक नहीं हो सकती हैं कि किस एंटी–वायरस एप्लिकेशन का उपयोग करना है।

(ञ) सॉफ्टवेयर चोरी स्वीकार्य नहीं है। उत्तराखंड राज्य डाटा सेंटर मशीनों पर पायरेटेड सॉफ्टवेयर स्थापित करना सॉफ्टवेयर चोरी का एक कार्य है। प्रतिलिपि बनाना – व्यक्तिगत उपयोग के लिए – उत्तराखंड राज्य डाटा सेंटर को लाइसेंस प्राप्त सॉफ़्टवेयर भी सॉफ़्टवेयर चोरी का एक कार्य है। उत्तराखंड राज्य डाटा सेंटर निम्नलिखित को स्वीकार नहीं करता है।

(ट) उन फोल्डरों को छोड़कर जहां कर्मचारियों को अनुमति दी जाती है, उत्तराखंड राज्य डाटा सेंटर कंप्यूटर नेटवर्क को ब्राउज़ करने की अनुमति नहीं है।

(ठ) सॉफ़्टवेयर एप्लिकेशन जिनमें ज्ञात भेद्यताएं हैं जो उत्तराखंड राज्य डाटा सेंटर कंप्यूटर नेटवर्क में सुरक्षा उल्लंघन के लिए एक स्थान खोल सकते हैं, उनका उपयोग नहीं किया जा सकता है। उत्तराखंड राज्य डाटा सेंटर में आईटी प्रबंधन के निर्देशों के तहत केवल अधिकृत कर्मचारी ही परीक्षण और मूल्यांकन उद्देश्यों के लिए ऐसे एप्लीकेशन का उपयोग कर सकते हैं। जैसे ही उद्देश्य समाप्त हो जाते हैं, ऐसे एप्लीकेशन को अनइंस्टॉल करने की आवश्यकता होती है और उनके कारण होने वाली किसी भी कमजोरियों को सुधारने और हटाने की आवश्यकता होती है।

221. प्रयोज्यता

यूकेएसडीसी के सभी हितधारकों की जिम्मेदारी है कि वे इस नीति का पालन करें और इसे अपने माध्यम से लागू करें।

222. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

अध्याय–32: आपदा पुनर्प्राप्ति (डीआर)

223. प्रयोजन

इस नीति का उद्देश्य आपदा पुनर्प्राप्ति (डी.आर.) योजनाओं और कार्यक्रमों के प्रावधान से जुड़ी गतिविधियों को परिभाषित करना है जो यूकेएसडीसी सूचना प्रणाली, डाटा, डाटाबेस और अन्य सूचना परिसंपत्तियों की रक्षा करते हैं।

224. नीति कथन और उद्देश्य

यह नीति उत्तराखंड राज्य डाटा सेंटर (यूकेएसडीसी) के सभी हितधारकों से संबंधित है, जिन्हें यूकेएसडीसी के संसाधनों और परिसंपत्तियों तक किसी भी समय अंतराल के लिए पहुंच प्रदान की जाती है।

225. नियंत्रण

1. यूकेएसडीसी अच्छी आपदा पुनर्प्राप्ति प्रबंधन पद्धतियों के अनुसार व्यापक आपदा वसूली योजना विकसित करेगा।
2. प्रौद्योगिकी आपदा पुनर्प्राप्ति गतिविधियों को व्यापार निरंतरता प्रबंधन प्रणाली (बीसीएमएस) के हिस्से के रूप में निष्पादित किया जाएगा, जो प्रौद्योगिकी आपदा पुनर्प्राप्ति कार्यक्रम का प्रबंधन और करता है जिसमें शामिल हैं:
   I. प्रौद्योगिकी आपदा पुनर्प्राप्ति गतिविधियों की योजना और डिजाइन, जिसमें प्रौद्योगिकी आपदा पुनर्प्राप्ति योजनाएं शामिल हैं।
   II. डी.आर. टीमों की पहचान, उनकी भूमिकाओं और जिम्मेदारियों को परिभाषित करना और यह सुनिश्चित करना कि वे किसी घटना का जवाब देने के लिए ठीक से प्रशिक्षित और तैयार हैं।
   III. डी.आर. व्यवसाय प्रभाव विश्लेषण हेतु अद्यतनों का निर्धारण।
   IV. डी.आर. जोखिम मूल्यांकन हेतु अद्यतनों का निर्धारण।
   V. कर्मचारियों और डी.आर. टीम के सदस्यों के लिए जागरूकता और प्रशिक्षण गतिविधियों की योजना और वितरण।
   VI. घटना प्रतिक्रिया गतिविधियों की योजना और डिजाइन
   VII. डी.आर. योजना अभ्यास का आयोजन और निष्पादन।
   VIII. यह सुनिश्चित करने के लिए कि सभी योजनाएं अद्यतित हैं और उपयोग के लिए तैयार हैं, डी.आर. कार्यक्रम/योजना अनुरक्षण गतिविधि को डिजाइन और कार्यान्वित करना।
   IX. डी.आर. कार्यक्रम और योजनाओं के लिए सतत सुधार गतिविधियों की योजना बनाना और उनका कार्यान्वयन।
3. सभी डी.आर. योजनाओं के लिए आवश्यकताओं को निर्धारित करने के लिए एक औपचारिक जोखिम मूल्यांकन (आर.ए.) और व्यावसायिक प्रभाव विश्लेषण (बी.आई.ए.) किया जाएगा; आर.ए. और बी.आई.ए. को यह सुनिश्चित करने के लिए कम से कम सालाना अद्यतन किया जाना चाहिए कि वे व्यवसाय और इसकी प्रौद्योगिकी आवश्यकताओं के अनुरूप हैं।

4. बी.आई.ए. और आर.ए. में परिभाषित विशिष्ट तकनीकी घटनाओं पर प्रतिक्रिया देने के लिए रणनीतियों की पहचान की जाएगी, और व्यक्तिगत डी.आर. योजनाओं को विकसित करते समय उनका उपयोग किया जाएगा।
5. आपदा वसूली योजनाओं में प्रमुख व्यावसायिक गतिविधियों के अनुसार सिस्टम, नेटवर्क, डाटाबेस और डाटा सहित महत्वपूर्ण तकनीकी तत्वों को संबोधित किया जाएगा।
6. आपदा वसूली योजनाओं का समय–समय पर एक उपयुक्त वातावरण में परीक्षण किया जाएगा ताकि यह सुनिश्चित हो सके कि सिस्टम, नेटवर्क, डाटाबेस और अन्य बुनियादी ढांचे के तत्वों को पुनर्प्राप्त किया जा सकता है और आपातकालीन स्थितियों में सामान्य स्थिति के रूप में एक व्यवसाय में वापस किया जा सकता है। और यह कि यूकेएसडीसी प्रबंधन और कर्मचारी समझते हैं कि योजनाओं को कैसे क्रियान्वित किया जाना है और साथ ही उनकी भूमिकाएं और जिम्मेदारियां भी हैं।
7. सभी कर्मचारियों को आपदा वसूली कार्यक्रम और योजनाओं और किसी घटना के दौरान उनकी अपनी भूमिकाओं और जिम्मेदारियों से अवगत कराया जाना चाहिए।
8. प्रौद्योगिकी आपदा वसूली योजनाओं और अन्य दस्तावेजों को अद्यतित रखा जाना है और मौजूदा और बदलती परिस्थितियों को प्रतिबिंबित करेगा।

226. प्रयोज्यता

यूकेएसडीसी के सभी हितधारकों की जिम्मेदारी है कि वे इस नीति का पालन करें और इसे अपने माध्यम से लागू करें।

227. प्रवर्तन एवं व्याख्या

कोई भी हितधारक, जो इस नीति का उल्लंघन करता है, विधि, जिसमें आईटी अधिनियम 2008 (संशोधन) धारा 43ए तथा 72ए के तहत आईटी एक्ट 2008 के रूप में संदर्भित है, के अनुसार उचित अनुशासनात्मक कार्रवाई के अधीन होगा।

(शैलेश बगौली)
सचिव।