अध्याय-4

सूचना प्रणाली सुरक्षा

अध्याय-4

सूचना प्रणाली सुरक्षा

4.1 परिचय

परम्परागत रूप से, सरकार के पास उपलब्ध जानकारी को अपने पूरे जीवनचक्र जैसे सृजन, भंडारण, पहुँच, संशोधन, वितरण और नष्ट करने के दौरान कागज के अभिलेख में रखकर सुरक्षित रूप से प्रबंधित किया जाता रहा है। तथापि, पारदर्शिता और विश्वसनीयता के साथ-साथ कुशल सेवा वितरण आउटलेट के माध्यम से आम आदमी के लिए स्थानीय स्तर पर सभी सरकारी सेवाओं को सुलभ बनाने के लिए सरकार ने सूचना के इलेक्ट्रॉनिक प्रारूपों का उपयोग करने की दिशा में लगातार तरक्की की है।

आई एफ एम एस एक वेब-आधारित प्रणाली है, जो सरकारी लेन-देन के भुगतान, लेखांकन और मिलान हेतु जो मौजूदा विभिन्न स्टैंडअलोन प्रणालियों को एकीकृत करता है। आई एफ एम एस, डेटा संग्रहण के एकल बिंदु की परिकल्पना करता है; इसलिए जानकारी की अखंडता और शुद्धता सुनिश्चित करना अत्यधिक महत्वपूर्ण है। चूँकि कोषागार के लेन-देन बहुत ही संवेदनशील स्वरूप के होते हैं इसलिए यह आवश्यक है कि ऐसे डेटा और लेन-देन की सुरक्षा, स्थिरता और अखंडता को सभी स्तरों पर बनाए रखा जाना चाहिए।

4.2 लेखापरीक्षा निष्कर्ष

उत्तराखण्ड में, आई एफ एम एस 01 अप्रैल 2019 से लागू किया गया था। इसे वर्तमान में निदेशालय कोषागार पेंशन एवं हकदारी (डी टी पी ई) के परिसर में स्थित एफ डी सी के माध्यम से संचालित किया जा रहा था। एफ डी सी के संयुक्त भौतिक निरीक्षण और आई एफ एम एस की प्रणाली समीक्षा के दौरान, लेखापरीक्षा द्वारा आई एफ एम एस और सेटअप में निम्नलिखित **(तालिका-4.1)** विशेषताओं को स्थापित और कार्यरत पाया गया:

तालिका-4.1: एफ डी सी के संयुक्त निरीक्षण के दौरान पाई गई अवलोकन की सूची

क्र.सं.	मापदण्ड	लेखापरीक्षा अवलोकन
1.	भौतिक पहुँच नियंत्रण	एफ डी सी के संयुक्त निरीक्षण के दौरान लेखापरीक्षा में पाया गया कि • बायोमैट्रिक डोर लॉक उपकरणों के माध्यम से एफ डी सी तक भौतिक पहुंच को प्रतिबंधित किया गया था। • सर्वर रूम को त्रिस्तरीय बायोमैट्रिक सुरक्षा के साथ सुरक्षित किया गया था तथा केवल अधिकृत लोगों को ही सर्वर रूम तक पहुँचने का अधिकार दिया गया था।

क्र.सं.	मापदण्ड	लेखापरीक्षा अवलोकन
		• निवारक उपाय जैसे अग्निशामक यंत्र, वातानुकूलित मशीनें इत्यादि अपने नियत स्थान पर थे। सर्वर रूम में धूल और बिखरा हुआ कोई भी सामान नहीं था।
2.	भेद्यता और खतरों की निगरानी	फोर्ट आई-गेट 2600एफ सीरीज फ़ायरवॉल के माध्यम से भेद्यता और खतरे की निगरानी के लिए घुसपैठ रोकथाम प्रणाली (आई पी एस), एंटी मॉलवेयर, फ़ायरवॉल एवं ई-मेल फ़िल्टरिंग एफ डी सी में स्थापित थी और सिस्टम लॉग रिकॉर्ड किए जा रहे थे।
3.	डेटाबेस सुरक्षा	लेखापरीक्षा में पाया गया कि: • डेटाबेस सर्वर को यू के एस डब्ल्यू ए एन के प्राइवेट नेटवर्क में होस्ट की गई अलग समर्पित मशीन पर इन्स्टाल किया गया था। • त्रिस्तरीय कनेक्शन पद्धति अपनाई गई थी क्योंकि डेटाबेस के सभी कनेक्शन एप्लिकेशन/एकीकरण सर्वर के माध्यम से रूट किए गए थे। • डेटाबेस को केवल विश्वसनीय आई पी एड्रेस की अनुमति देने हेतु कॉन्फ़िगर किया गया था। • सभी उपयोगकर्ताओं के सत्रों को सिक्योर सॉकेट लेयर (एस एस एल) हैंडशेक के माध्यम से एन्क्रिप्ट किया गया था ताकि पारगमन में डेटा सुरक्षित रखा जा सके। • डेवलेपमेंट डाटाबेस/एप्लीकेशन को प्रॉडक्शन डाटाबेस/एप्लीकेशन से अलग रखा गया था।

4.2.1 एस टी क्यू सी से निष्पादन और गुणवत्ता लेखापरीक्षा ना करवाया जाना

मानकीकरण परीक्षण और गुणवत्ता प्रमाणन (एस टी क्यू सी) निदेशालय, इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार का एक संलग्न कार्यालय है जो परीक्षण, प्रशिक्षण, लेखापरीक्षा और प्रमाणन द्वारा सॉफ्टवेयर परीक्षण, सूचना सुरक्षा और आई टी सेवा प्रबंधन के लिए गुणवत्ता आश्वासन सेवाएं प्रदान करता है।

लेखापरीक्षा में पाया गया कि आई एफ एम एस के लागू होने से पूर्व एस टी क्यू सी से निष्पादन एवं गुणवत्ता लेखापरीक्षा कराने की ज़िम्मेदारी चयनित निविदादाता[1] की थी। लेकिन एस टी क्यू सी से आवश्यक प्रमाणन कराये बिना ही सिस्टम को 01 अप्रैल 2019 से लागू कर दिया गया। लेखापरीक्षा के दौरान, डी टी पी ई ने यह भी स्वीकार किया कि आई एफ एम एस के उपयोगकर्ता धीमी गति का सामना कर रहे थे। अतः आवश्यक एस टी क्यू सी प्रमाणन के अभाव में, आई एफ एम एस में गुणवत्ता और निष्पादन के मुद्दों के जोखिम से इनकार नहीं किया जा सकता था।

[1] मै इंडस वेब सोल्यूशन, प्राइवेट लिमिटेड।

शासन ने तथ्यों को स्वीकारते हुए अपने उत्तर (अगस्त 2023) में बताया कि डिजिटलीकरण का कुछ कार्य प्रगतिशील था जिसे 2023-24 तक पूर्ण कर लिया जायेगा। डिजिटलीकरण का कार्य पूर्ण होने के उपरांत एस टी क्यू सी कराया जाएगा। उत्तर स्वीकार्य नहीं था क्योंकि वेंडर को पहले ही प्रदेय 'एस टी क्यू सी से निष्पादन एवं गुणवत्ता लेखापरीक्षा' हेतु भुगतान किया जा चुका था तथा उसके साथ किया गया अनुबंध 31 मार्च 2023 को समाप्त हो चुका था।

4.2.2 सूचना प्रणाली (आई एस) सुरक्षा में प्रणालीगत कमियाँ

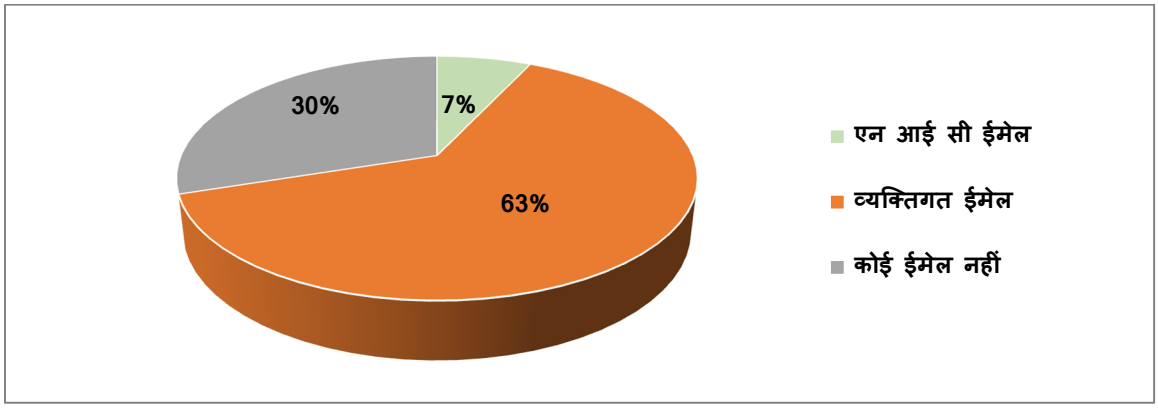
प्रणाली समीक्षा के दौरान, लेखापरीक्षा द्वारा निम्नलिखित कमियाँ पाई गईं:

(i) डी डी ओ द्वारा व्यक्तिगत ई-मेल आई डी का प्रयोग किया जाना

उत्तराखण्ड शासन के निर्देशों के अनुसार, "आई एफ एम एस पोर्टल पर सरकारी कार्य करने हेतु तथा सूचनाओं के आदान-प्रदान हेतु समस्त डी डी ओ को राज्य एन आई सी द्वारा उपलब्ध करायी गयी सरकारी ई-मेल का प्रयोग करना होगा। आई एफ एम एस पर कार्य करने के लिए व्यक्तिगत ई-मेल का प्रयोग कड़ाई से निषिद्ध है"। लेखापरीक्षा में पाया गया कि 4586 में से 2912 (63 *प्रतिशत*) डी डी ओ उनके व्यक्तिगत ई-मेल आई डी के साथ पंजीकृत थे क्योंकि आई एफ एम एस में यह सुनिश्चित करने के लिए कि डी डी ओ केवल सरकारी ई-मेल आई डी के माध्यम से आई एफ एम एस में पंजीकरण करे, इसके लिए कोई नियंत्रण उपलब्ध नहीं था। यह एक सम्भावित सुरक्षा जोखिम पैदा करता था क्योंकि सरकारी डेटा को सरकारी नियंत्रण के बाहर सर्वरों में संग्रहित किया जा रहा था।

बहिर्गमन गोष्ठी (जून 2023) के दौरान, लेखापरीक्षा अवलोकनों को स्वीकारते हूए शासन ने अवगत कराया कि अवशेष डी डी ओ हेतु सरकारी ई-मेल आई डी बनाने के लिए एक अभियान शुरू किया जाएगा और बाद में डी डी ओ की ई-मेल आई डी आई एफ एम एस में अद्यतन कर दी जायेगी।

चार्ट-5: ई-मेल आई डी का प्रयोग



(ii) ऑडिट ट्रेल्स का अभाव

ऑडिट ट्रेल (जिसे ऑडिट लॉग भी कहा जाता है) एक सुरक्षा-प्रासंगिक कालानुक्रमिक रिकॉर्ड, रिकॉर्ड का सेट तथा/अथवा रिकॉर्ड का गंतव्य और स्रोत है जो किसी भी समय किसी विशिष्ट ऑपरेशन, प्रक्रिया, घटना या उपकरण को प्रभावित करने वाली गतिविधियों के अनुक्रम के दस्तावेजी सबूत प्रदान करता है। प्रणाली समीक्षा के दौरान, लेखापरीक्षा ने पाया कि आई एफ एम एस में ऑडिट ट्रेल्स को शामिल नहीं किया गया था जिसके कारण आई एफ एम एस के माध्यम से किए गए परिवर्तनों का विवरण फ्रंट-एंड से पता नहीं लगाया जा सकता था। उदाहरणार्थ: अस्वीकृति और बिल पर की गई अनुवर्ती कार्रवाइयों के विवरण सहित बिल का लाइफसाइकल बैक-एंड पर लॉग्स के रूप में कैप्चर किया जाता था लेकिन डी डी ओ उपयोगकर्ताओं हेतु फ्रंट-एंड पर उपलब्ध नहीं था।

शासन द्वारा इस तथ्य को स्वीकार किया गया कि ऑडिट ट्रेल फ्रंट-एंड पर नहीं दर्शाया जा रहा था तथा अवगत कराया (अगस्त 2023) कि ऑडिट ट्रेल हेतु प्रतिवेदन शीघ्र ही डी डी ओ को उपलब्ध करा दी जाएगी।

(iii) कमजोर पासवर्ड नीति

पासवर्ड नीति के अनुसार पासवर्ड अपर और लोअर केस वर्णों, अंकों और विराम चिह्नों के साथ-साथ अन्य वर्णों का संयोजन होना चाहिए। लेखापरीक्षा में पाया गया कि प्रणाली पासवर्ड बनाते समय लोअर केस के उपयोग को बाध्य नहीं कर रही थी।

शासन द्वारा तथ्यों को स्वीकारते हुए आश्वासन (अगस्त 2023) दिया गया कि भविष्य में इसका अनुपालन किया जायेगा।

(iv) लॉगिन के दौरान बायोमैट्रिक प्रमाणीकरण को लागू ना किया जाना

परियोजना के सॉफ्टवेयर रिक्वाइरमेंट स्पेसिफिकेशन (एस आर एस) के अनुसार, आहरण एवं वितरण कार्यालयों[2] तथा कोषागारों में पंजीकृत उपयोगकर्ताओं हेतु बायोमैट्रिक प्रमाणीकरण प्रणाली (फिंगरप्रिंट कैप्चर के रूप में) को आई एफ एम एस में लागू किया जाना था। तथापि, आई एफ एम एस के परिचालन के तीन साल बाद भी यह लागू नहीं किया गया था।

[2] डी डी ओ मुख्य रूप से एक फ्रंट-ऑफिस प्रकार का वेब एप्लिकेशन है जिसे वेब ब्राउज़र का उपयोग करके इंटरनेट पर एक्सस किया जा सकता है।

शासन द्वारा बायोमैट्रिक प्रमाणीकरण के महत्व को स्वीकार करते हुए अवगत कराया (अगस्त 2023) गया कि आधार के साथ एकीकरण प्रस्तावित था। इसके लागू होने के उपरांत, लॉगिन के समय उपयोगकर्ताओं द्वारा आधार आधारित बायोमैट्रिक प्रमाणीकरण किया जाएगा।

(v) नेटवर्क सुरक्षा

लेखापरीक्षा में पाया गया कि आई एफ एम एस को सूचना प्रौद्योगिकी विकास एजेंसी (आई टी डी ए), देहरादून द्वारा प्रबंधित यू के एस डब्ल्यू ए एन पर संचालित किया जा रहा था। डी टी पी ई और आई टी डी ए को अनुरोध किए जाने के बावजूद, यू के एस डब्ल्यू ए एन के नेटवर्क सुरक्षा लेखापरीक्षा प्रमाण पत्र लेखापरीक्षा को उपलब्ध नहीं करवाए गए। लेखापरीक्षा प्रमाणपत्रों के अभाव में, लेखापरीक्षा, आई एफ एम एस की नेटवर्क सुरक्षा का पता नहीं लगा सका।

4.2.3 बिज़नेस कंटिन्युटी प्लान (बी सी पी) का अभाव

आई एफ एम एस परियोजना के अंतर्गत बी सी पी तैयार कर लागू करना एक प्रमुख कार्य था। बी सी पी यह सुनिश्चित करता है कि आपदाओं और अन्य आपातकालीन घटनाओं की परिस्थिति में प्रणाली सुचारू रूप से चलती रहे और निश्चित समय सीमा के अंदर अपने संचालन को फिर से शुरू करे। लेखापरीक्षा में पाया गया कि आई एफ एम एस लागू होने के चार साल बाद भी बी सी पी तैयार कर अपनाया नहीं गया था। इसके अभाव में, कर्मचारी/उपयोगकर्ता, व्यवधान/आपदाओं की स्थिति में पालन की जाने वाली प्रक्रिया से अनजान थे। उन्हें आपातकालीन स्थितियों को रोकने, कम करने और प्रतिक्रिया देने हेतु प्रशिक्षित भी नहीं किया गया था।

बहिर्गमन गोष्ठी (जून 2023) के दौरान, बी सी पी की महत्ता को स्वीकार करते हुए शासन द्वारा, डी टी पी ई को शीघ्रातिशीघ्र बी सी पी तैयार किए जाने हेतु निर्देशित किया गया।

उत्तर स्वीकार्य नहीं था क्योंकि बी सी पी तैयार करने की जिम्मेदारी वेंडर की थी जिसे इसके लिए पहले ही भुगतान किया जा चुका था। बी सी पी के अभाव में, व्यवधानों/ आपदाओं की दशा में आई एफ एम एस की व्यवसायिक निरंतरता को जोखिम था।

4.2.4 डिजास्टर रिकवरी साइट का स्थापित ना किया जाना

डिजास्टर रिकवरी (डी आर) का उद्देश्य विभाग को महत्वपूर्ण विनाशकारी घटनाओं के प्रभाव से बचाना है। यह विभागों को आपदा के बाद मिशन-महत्वपूर्ण कार्यों को जल्दी से

फिर से शुरू करने में मदद करता है। विभिन्न सम्भावित आपदाएं जो हो सकती हैं- मानव त्रुटि, महामारी, बिजली का ना होना, आग या विस्फोट आदि। डी आर साइट के लिए दूरी, आपदा के प्रकारों के आधार पर भिन्न-भिन्न हो सकती है- जैसे भूकम्प, बाढ़, आतंकवादी हमले, इत्यादि। विभाग को एक ऐसी डी आर साइट चुननी चाहिए जो इसके व्यवसायिक मॉडल और नियामक आवश्यकताओं के अनुरूप हो।

लेखापरीक्षा में पाया गया कि परियोजना की डी पी आर के अनुसार, डी आर साइट को स्टेट डेटा सेंटर (एस डी सी) आई टी डी ए में स्थापित किया जाना था। उसी डी पी आर में, यह परिकल्पना की गई थी कि आई टी डी ए में एस डी सी के चालू हो जाने के बाद, एफ डी सी[3] में समस्त आई टी बुनियादी ढाँचे और आई एफ एम एस संचालन को एस डी सी में स्थानांतरित कर दिया जाएगा और पूर्व व्यवस्था एक आर्काइवल साइट के रूप में कार्य करेगा। वित्त सचिव की अध्यक्षता में डी टी पी ई, एन आई सी और आई टी डी ए के साथ दिनांक 03 दिसम्बर 2021 को हुई बैठक मे एस डी सी में डी आर साइट बनाने के प्रस्ताव को पुनः दोहराया गया था।

लेखापरीक्षा ने पाया कि डी पी आर के दो प्रावधान परस्पर विरोधाभासी थे क्योंकि आई एफ एम एस संचालन को एफ डी सी से एस डी सी में स्थानांतरित करने के बाद एस डी सी, डी आर साइट के रूप में कार्य नहीं कर सकता था क्योंकि परिभाषा के अनुसार डी आर साइट भौगोलिक रूप से अलग स्थान पर होनी चाहिए थी। इसके अतिरिक्त, एफ डी सी और एस डी सी दोनों, लगभग 6.5 किलोमीटर की दूरी पर थे तथा आपदाओं (भूकम्पीय क्षेत्र IV) हेतु संवेदनशील क्षेत्र में एक-दूसरे के पास स्थित थे। हाल ही में, 25 अगस्त 2021 को बादल फटने से क्षेत्र में अचानक बाढ़ जैसी स्थिति उत्पन्न हो गई थी। इस प्रकार, 01 अप्रैल 2019 से आई एफ एम एस लागू होने के बावजूद भी, डी आर साइट स्थापित करने हेतु कोई प्रयास नहीं किए गए थे, जिसके अभाव में शासन के महत्वपूर्ण वित्तीय संचालन किसी भी आपदा की दशा में असुरक्षित थे।

बहिर्गमन गोष्ठी (जून 2023) के दौरान, शासन द्वारा डी आर साइट के महत्व को स्वीकार करते हुए अवगत कराया गया कि वर्तमान में एफ डी सी में होस्ट किए गए आई एफ एम एस एप्लिकेशन को आई टी डी ए में स्थित एस डी सी में स्थानांतरित

[3] डी पी आर में, एकीकृत डेटा सेंटर

करने की योजना थी। इसके अतिरिक्त, आई टी डी ए, एस डी सी में होस्ट की गई सभी एप्लीकेशन्स के लिए एक 'फार' डी आर साइट बनाने की योजना बना रहा था।

उत्तर स्वीकार्य नहीं था क्योंकि देहरादून भूकम्पीय क्षेत्र में स्थित है और यहाँ पर भूकम्प, बाढ़, बादल फटने आदि जैसी प्राकृतिक आपदाओं की आशंका बनी रहती है। एक कार्यात्मक डी आर साइट के अभाव में, आपदाओं की दशा में आई एफ एम एस की व्यवसायिक निरंतरता को खतरा था।

4.2.5 बैकअप तथा रिकवरी कंट्रोल्स

राष्ट्रीय सूचना सुरक्षा नीति और दिशा-निर्देश, 2014 के अनुसार संगठन को यह अवश्य सुनिश्चित करना चाहिए कि समस्त ऑपरेशनल डेटा के लिए बैकअप प्रतियाँ रखी जाएं ताकि यदि वे अनजाने में नष्ट हो जाएँ अथवा खो जाएँ, तो ऑपरेशनल डेटा को पुनः स्थापित किया जा सके। इसके अतिरिक्त, बैकअप नीति के अनुसार सूचना और सॉफ्टवेयर की बैकअप प्रतियां ली जानी चाहिएँ तथा उनका नियमित रूप से परीक्षण किया जाना चाहिए।

लेखापरीक्षा में पाया गया कि आई एफ एम एस में सृजित डेटा को आई टी डी ए के एस डी सी में रियल टाइम के आधार पर रेप्लीकेट किया जा रहा था। डी टी पी ई के एफ डी सी में बैकअप निर्धारित था जिसमें डेटा स्कीमा का दैनिक बैकअप तथा प्रत्येक 15 दिनों के बाद पूर्ण बैकअप लिया जा रहा था। हालाँकि, विभाग द्वारा आई एफ एम एस के लागू होने के तीन साल के बाद भी बैकअप पॉलिसी नहीं बनाई गई थी और ना ही बैकअप डेटा से रिस्टोर करके प्रणाली का परीक्षण किया गया था। इसके अतिरिक्त, विभाग द्वारा डेटा रिटेंशन पीरियड निर्धारित नहीं किया गया था जिसके अभाव में डेटा बढ़ता जा रहा था तथा रेस्पोंस टाइम में बढ़ोत्तरी के कारण प्रणाली की परफ़ोर्मेंस को प्रभावित कर सकता है।

शासन द्वारा अपने उत्तर (अगस्त 2023) में इस तथ्य को स्वीकार किया गया कि बैकअप नीति तैयार नहीं की गई थी, परंतु डेटाबेस एडमिनिस्ट्रेटर (डी बी ए) द्वारा दैनिक, मासिक, इंक्रीमेंटल और पूर्ण बैकअप लिए जा रहे थे। शासन ने अपने जवाब में दावा किया कि बैकअप गतिविधियों की मासिक आधार पर समीक्षा और परीक्षण किया गया था, हालाँकि, अपने दावों को स्थापित करने हेतु कोई भी अभिलेख लेखापरीक्षा को उपलब्ध नहीं करवाए गये थे।

4.2.6 आउटसोर्स कर्मियों द्वारा महत्वपूर्ण वित्तीय डेटा का प्रबंधन किया जाना

एफ डी सी के प्रबंधन हेतु, डी टी पी ई ने काम की संवेदनशीलता और इसमें शामिल वित्तीय प्रभावों को देखते हुए तकनीकी रूप से कुशल नियमित कर्मियों को तैनात करने की आवश्यकता का हवाला देते हुए सात पदों/तकनीकी कैडर की मंजूरी की माँग की थी। शासनादेश दिनांक 12 सितंबर 2019 के अनुसार, उत्तराखण्ड शासन द्वारा तीन तकनीकी पदों[4] की मंजूरी दी गई थी और डी टी पी ई को उपरोक्त तकनीकी कैडर में सीधी भर्ती से पहले सेवा नियमावली तैयार करने और 29 फरवरी 2020 से पहले सृजित पदों को भरने हेतु निर्देशित किया गया था।

लेखापरीक्षा में पाया गया कि आवश्यक सेवा नियमावली तैयार करने और स्वीकृत पदों पर सीधी भर्ती करने के बजाय, एफ डी सी में सभी तकनीकी कर्मचारियों को आउटसोर्स किया गया था और अनुबंध के आधार पर काम पर रखा गया था। यह न केवल संविदा कर्मचारियों पर निर्भरता पैदा करता था, अपितु इसमें महत्वपूर्ण सुरक्षा जोखिम भी सम्मिलित थे क्योंकि वित्तीय लेन-देन और व्यक्तिगत डेटा सहित महत्वपूर्ण डेटाबेस को संविदा कर्मचारियों द्वारा प्रबंधित किया जा रहा था। यह 'सम्भावित दुरुपयोग को प्रतिबंधित करने और संग्रहित डेटा की सुरक्षा करने' के उद्देश्य को विफल करता था जिसके लिए शासन द्वारा तकनीकी कैडर की मंजूरी दी गई थी।

शासन ने अपने उत्तर (अगस्त 2023) में बताया कि संविदा कर्मचारी, डोमेन टीम की कड़ी निगरानी में कार्य करते थे जिसे सरकारी कर्मचारियों द्वारा संचालित किया जाता था। अधिकांश संविदा कर्मी पिछले दस वर्षों से एफ डी सी में कार्यरत थे। अतिरिक्त तकनीकी संसाधनों को रखने के प्रयास किए जा रहे थे जो ना केवल आई एफ एम एस के रख-रखाव और संवर्धन में मदद करेंगे, अपितु मौजूदा संसाधनों के बैकअप के रूप में कार्य करेंगे। भविष्य में, स्थायी तकनीकी कर्मचारियों की सेवा नियमावली तैयार करने के बाद उनकी नियुक्ति हेतु सरकार को अधियाचन भी भेजा जाएगा।

4.2.7 अभिलेखीकरण और नीतियों का अभाव

वेब एप्लीकेशन की सुरक्षा सभी हितधारकों के लिए सर्वोपरि चिंता का विषय है। भारत सरकार द्वारा वेबसाइटों हेतु जारी दिशा-निर्देशों के अनुसार विभाग को वेबसाइट से

[4] दो सीधी भर्ती के पद (सिस्टम एड्मिनिस्ट्रेटर एवं डेटाबेस एड्मिनिस्ट्रेटर) तथा एक आउटसोर्स पद (सीनियर सॉफ्टवेअर इंजीनियर)

सम्बंधित विभिन्न सुरक्षा मुद्दों को सम्बोधित करने के लिए एक सुरक्षा नीति तैयार करनी चाहिए। इसलिए, आई एफ एम एस के उचित काम-काज हेतु एक अच्छी तरह से प्रलेखित सुरक्षा नीति की आवश्यकता थी।

लेखापरीक्षा में पाया गया कि विभाग द्वारा आई टी परिसम्पत्तियों, सॉफ्टवेयर और डेटा, बैकअप, डेटा रिटेंशन और डिस्पोजल, घटना रिपोर्टिंग, ई-मेल, पासवर्ड इत्यादि की सुरक्षा हेतु कोई आई टी सुरक्षा नीति तैयार नहीं की गयी थी। प्रलेखित सुरक्षा नीति के अभाव में प्रत्येक उपयोगकर्ता अपने तरीके से ऐसे मुद्दों को सँभालने के लिए स्वतंत्र था जोकि आई एफ एम एस की आई टी सुरक्षा के लिए जोखिम पैदा कर सकते थे।

शासन द्वारा तथ्यों को स्वीकारते हुए अवगत (अगस्त 2023) कराया गया कि आई एफ एम एस को एस डी सी में स्थानांतरित किया जा रहा था और बुनियादी ढांचे, नेटवर्क, पासवर्ड इत्यादि के सम्बंध में एस डी सी की आई टी नीति को अपनाया जाएगा। अन्य नीतियाँ, जैसे बी सी पी, डी आर नीति आदि को डी टी पी ई द्वारा नियत समय में तैयार किया जायेगा।

4.3 आई एफ एम एस के उपयोगकर्ताओं द्वारा प्रतिकूल प्रतिक्रिया

लेखापरीक्षा द्वारा डी डी ओ तथा कोषागारों में आई एफ एम एस के उपयोगकर्ताओं से प्रतिक्रिया प्राप्त करने हेतु एक ऑनलाइन सर्वेक्षण किया गया। सर्वेक्षण के दौरान लगभग 370 प्रतिक्रियाएं प्राप्त हुईं। सर्वेक्षण में उपयोगकर्ताओं द्वारा लॉगिन, ओ टी पी प्राप्त होने में देरी, हेल्पडेस्क से सपोर्ट में देरी या खराब सपोर्ट,वेबसाइट की धीमी गति, सर्वर डाउन, बिल सृजन और लेखांकन, प्रशिक्षण की कमी, उपयोगकर्ता-अनुकूलता की कमी, विभिन्न प्रतिवेदनों और मॉड्यूलों में समस्या, लेगेसी डेटा की अनुपलब्धता, वर्कफ्लो, वेंडर अथवा पार्टी प्रबंधन, फ़ाइल-अपलोड साइज, अचानक लॉगआउट के बाद अनावश्यक 20 मिनट की प्रतीक्षा अवधि, हार्डकॉपी के कारण काम का दोहरापन, सेव-सेशन सक्रिय ना होना, जी पी एफ में विसंगति, वाउचर बनाने में देरी, जी एस टी के संदर्भ में ठेकेदारों के खातों का दोहरापन, वर्क्स मॉड्यूल और अन्य कई मुद्दों को रेखांकित किया गया।

शासन द्वारा आई एफ एम एस के उपयोगकर्ताओं द्वारा दी गई प्रतिक्रियाओं को स्वीकार करते हुए अवगत (अगस्त 2023) कराया गया कि कुछ मुद्दों की पहचान कर

उन्हें ठीक कर लिया गया था। प्रणाली के एस डी सी में स्थानांतरित हो जाने के बाद प्रणाली की धीमी गति से सम्बंधित मुद्दों का समाधान कर लिया जाएगा। अतिरिक्त तकनीकी कर्मचारियों की नियुक्ति के बाद अन्य मुद्दों को हल किया जाएगा।

4.4 निष्कर्ष

आई एफ एम एस एप्लिकेशन की सूचना सुरक्षा, स्वामियों के साथ-साथ एप्लीकेशन के उपयोगकर्ताओं के लिए सर्वोपरि चिंता का विषय है क्योंकि कोषागार लेन-देन स्वरूप से बहुत ही संवेदनशील होते हैं। लेखापरीक्षा में पाया गया कि एस टी क्यू सी से आवश्यक निष्पादन और गुणवत्ता प्रमाणन करवाए बिना ही आई एफ एम एस को लागू कर दिया गया। आई एफ एम एस में, डी डी ओ को उनके व्यक्तिगत ई-मेल आई डी के साथ पंजीकृत किया गया था, जिससे सुरक्षा जोखिम सम्भावित था। आई एफ एम एस के परिचालन के तीन साल बाद भी विभाग द्वारा बायोमैट्रिक प्रमाणीकरण को लागू नहीं किया गया था। लेखापरीक्षा प्रमाणपत्र के अभाव में आई एफ एम एस की नेटवर्क सुरक्षा सुनिश्चित नहीं की जा सकी। भूकम्पीय क्षेत्र में होने के बावजूद, विभाग द्वारा बी सी पी तैयार नहीं किया गया और ना ही कोई कार्यात्मक डी आर साइट स्थापित की गयी। बी सी पी/डी आर साइट के अभाव में आपदाओं की दशा में आई एफ एम एस की व्यवसायिक निरंतरता को जोखिम था। विभाग द्वारा कोई भी आई टी सुरक्षा नीति नहीं बनाई गई। प्रलेखित नीतियों के अभाव में, उपयोगकर्ता अपने तरीके से सुरक्षा सम्बंधी मुद्दों को संभालने के लिए स्वतंत्र थे जोकि आई एफ एम एस की आई टी सुरक्षा के लिए जोखिम पैदा कर सकते थे।

4.5 संस्तुतियाँ

- ***विभाग द्वारा आई एफ एम एस में अवशेष डी डी ओ हेतु सरकारी ई-मेल आई डी बनाने और अद्यतन करने की प्रक्रिया में तेजी लानी चाहिए।***
- ***विभाग द्वारा बिजनेस कंटिन्युटी प्लान तैयार किया जाना चाहिए तथा डिजास्टर रिकवरी साइट स्थापित की जानी चाहिए ताकि यह सुनिश्चित किया जा सके कि प्रणाली सुचारू रूप से चलती रहे तथा आपदाओं और अन्य आपातकालीन घटनाओं की दशा में निश्चित समय अवधि के भीतर अपना संचालन फिर से शुरू कर सके।***

- ***विभाग द्वारा नियमित आधार पर बैकअप पुनर्स्थापना गतिविधि की समीक्षा और परीक्षण किया जाना चाहिए ताकि अनजाने में नष्ट हो जाने अथवा खो जाने पर डेटा को पुनर्स्थापित किया जा सके।***
- ***विभाग द्वारा आई टी परिसम्पत्तियों, सॉफ्टवेयर और डेटा, बैकअप, डेटा रिटेंशन और डिस्पोजल आदि की सुरक्षा हेतु एक आई टी सुरक्षा नीति तैयार की जानी चाहिए।***

देहरादून
दिनांक: 10 अप्रैल 2024

(प्रवीन्द्र यादव)
प्रधान महालेखाकार (लेखापरीक्षा),
उत्तराखण्ड

प्रतिहस्ताक्षरित

नई दिल्ली
दिनांक: 26 अप्रैल 2024

(गिरीश चंद्र मुर्मू)
भारत के नियंत्रक-महालेखापरीक्षक