स्वचालित भन्सार जाँचपास प्रणाली (आशिकुडा)को उपयोग स्थितिको मूल्यांकन

परिच्छेद-१ : पृष्ठभूमि

१.१ स्थापना, उद्देश्य र कार्यक्षेत्र : भन्सार विभाग र अर्न्तगतका भन्सार कार्यालयहरुमा प्रयोग भएको भन्सार जाँचपास व्यवस्थालाई सूचना प्रविधिमा आधारित बनाउने उद्देश्यले सन् १९९६ देखि स्वचालित भन्सार जाँचपास (आशिकुडा) प्रणाली प्रयोगमा रहेको थियो । यसबाट भन्सार जाँचपास प्रणाली पूर्णरुपमा स्वचालनमा आउन नसकेकोले सन् २०१६ को अन्तर्राष्ट्रिय भन्सार दिवसको अवसरमा आसिकुडाको नयाँ भर्सन आसिकुडा वर्ल्ड कार्यान्वयनमा ल्याई हाल नेपाल भन्सार जाँचपास प्रणाली (नेपाल कस्टम अटोमेटेड सिस्टम) नेपाली नामाकरण गरिएको छ । यो प्रणालीले भन्सार जाँचपास प्रणालीलाई सरल, सहज, र अन्तराष्ट्रियस्तरको बनाउन भन्सार परिसरमा मालबाहक सवारीको प्रवेश, दर्ता, मूल्याङ्कन, कर तथा महशुल भुक्तानी र बर्हिगमनसम्मका सम्पूर्ण जाँचपास गर्ने गरिएको छ । यस प्रणालीको सफल कार्यान्वयनकोलागि आवश्यक हार्डवेयर, नेटवर्क इक्युपमेण्ट र सफ्टवेयरहरुको व्यवस्था भएको र भन्सार विभागमा डाटा सेन्टरको स्थापना हुने र भन्सार कार्यालयहरुमा यसै प्रणाली अनुसार आयात/निर्यातको तथ्याङ्क अभिलेखन तथा भन्सार जाँचपास हुने गरेको छ । यसको कार्यक्षेत्र भन्सार विभाग र अर्न्तगतका भन्सार कार्यालयहरुमा रहेको छ ।

१.२ कानूनी व्यवस्था : भन्सार ऐन, २०६३ तथा नियमावली, २०६४, विद्युतीय कारोवार ऐन, २०६३ तथा नियमावली, २०६४

१.३ नीतिगत व्यवस्था : राष्ट्रिय विद्युतीय शासन गुरुयोजना, सरकारी निकायको वेभ साईट निर्माण तथा व्यवस्थापन सम्बन्धी निर्देशिका, २०६८, सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१, सूचना तथा सञ्चार प्रविधि नीति, २०७२ ।

१.४ चालु वर्षको वजेट वक्तव्यमा उल्लेख भएका प्रमुख व्यवस्था :

- सूचना तथा सञ्चार प्रविधिकालागि आ.व. २०७४।७५ मा रु.४ अर्ब ९८ करोड विनियोजनको व्यवस्था,
- सरकारी निकायबाट प्रकाशित सामग्री, सूचना तथा निर्णयहरु एकीकृत रुपमा विद्युतीय माध्यमबाट समेत उपलब्ध गराउने गरी सूचना विभागमा सूचना बैंकको स्थापना गरिने व्यवस्था ।

परिच्छेद-२ : लेखापरीक्षणको उद्देश्य, क्षेत्र, पद्धति र सीमा

२.१ उद्देश्य : सरकारी निकायहरुबाट सञ्चालन हुने कार्य सञ्चालन गर्न प्रयोगमा ल्याईएका सूचना प्रविधि प्रणालीको वैधानिकता र तिनको उपयोगको स्थिति मूल्यांकनकालागि राष्ट्रिय विद्युतीय शासन गुरुयोजना र यसको कार्यन्वयन पक्षको अध्ययन गरि निकायको कार्यसम्पादनमा उपयोग गरिएको सूचना प्रविधि सफ्टवेयरको दुरुस्तता, पूर्णता र नियमितता एवं प्रमाणीकरण पद्धतिमा परीक्षण गरि नियन्त्रण पद्धति, तथ्याङ्कको बिश्वसनियता, एप्लीकेशन प्रणालीको उपयुक्तता, प्रविधिको प्रयोग, सूचना प्रविधि पूर्वाधार, जनशक्ति व्यवस्थापन, सफ्टवेयरको प्रभावकारीता ,उपयोग प्रणालीको दक्षता, सुचना प्रणालीको गोप्यता, उपलब्ध हुने सूचनाको विश्वसनीयता तथा सूरक्षा प्रणाली मूल्यांकन गर्ने सिलसिलामा सूचनाको विश्वसनीयता, एप्लिकेशन प्रणालीको उपयुक्तता, प्रविधिको उपयोग, सूचनाको निष्पक्षता, निष्ठा, एंव कानुनी प्रावधानहरुसँगको परिपालनाको जाँच गर्नु सूचना प्रविधि लेखापरीक्षणको उद्देश्य रहेको छ ।

२.२ लेखापरीक्षणको क्षेत्र : यस लेखापरीक्षणले भन्सार विभाग र अन्तर्गतका कार्यालयहरुको सूचना प्रविधि संयन्त्र र विशेष गरी यस विभागमा प्रयोगमा ल्याईएको सफ्टवेयरलाई समेटेको छ ।

२.३ पद्धति : लेखापरीक्षण योजनामा उल्लेखित विधि एवं प्रक्रिया अनुरुप लेखापरीक्षण गरिने निकायको सूचना प्रविधि वातावरणको अध्ययन, जोखिम क्षेत्रको पहिचान गरि सम्बन्धित निकायबाट विद्युतीय तथ्याङ्क प्राप्त गरि उपयुक्त लेखापरीक्षण विधिद्धारा त्यसको सुनिश्चितता यकिन गरिएको छ । यसका अलावा सूचना प्रविधिमा संलग्न जनशक्तिसँगको छलफल र तथ्याङ्क परीक्षण तथा विश्लेषण गरिएको छ ।

२.४ सीमा : नमुना छनौट, मानवीय त्रुटि, कारोबार र प्रणालीको जटिलता एंव अनिश्चतता, पेशागत विवेकको प्रयोग, समयको कमी, समयमै सूचना प्राप्त नहुने, त्रुटी वा जालसाजी पत्ता नलाग्ने ईत्यादि लेखापरीक्षणका सिमितताका रुपमा रहेका छन् ।

परिच्छेद-३ : लेखापरिक्षणवाट देखिएका व्यहोरा :

३.१ सूचना प्रविधि निर्देशक समिति : सूचना प्रविधि सम्बन्धमा देखिएका नवीन अवधारणा तथा आन्तरिक रुपमा देखिएका समस्या तथा चुनौती उपर निर्णय लिनकोलागि विभागमा सूचना प्रविधि निर्देशक समिति गठन गरिनु पर्दछ । विभागले मिति २०७१।७।२८ मा निर्देशक समिति तथा समन्वय समिति समिति गठन गरेता पनि हालसम्म कुनै काम गरेको छैन । जसले गर्दा सूचना प्रविधि सम्बन्धमा देखिएका प्राविधिक समस्या तथा चुनौती उपर तत्काल निर्णय लिन असहज भई सूचना प्रविधि कार्यमा रोकावट आउन सक्दछ ।

३.२ वार्षिक तथा रणनैतिक योजना : विभागले स्वचालित भन्सार जाँचपास प्रणाली(आशिकुडा) सम्बन्धमा वार्षिक रुपमा गरिने कार्यको लागि वार्षिक तथा रणनैतिक योजना तयार गरेको हुनुपर्दछ । विभागमा सो सम्बन्धमा विशेष रुपमा सूचना प्रविधि सम्बन्धि वार्षिक तथा रणनैतिक योजना तयार नगरी विभागको समष्टिगत ५ वर्षे रणनैनिक योजनामा समावेश गरेको छ । जसले गर्दा विभागले वार्षिक रुपमा सूचना प्रविधि सम्बन्धमा के कस्ता कार्यहरु गर्नुपर्ने हो सो सम्बन्धमा स्पष्टता भएको देखिदैन ।

३.३ सूचना प्रविधि नीति : विभागमा प्रयोग भएको सफ्टवेयर सुरक्षा सम्बन्धमा सूचना प्रविधि नीति, सूरक्षा नीति, व्यवसाय निरन्तरता नीति, डिजास्टर रिकभरी नीति, हार्डवेयर नीति, सफ्टवेयर नीति, तथ्याङ्कहरुको गोपनियता नीति, ब्याकअप नीति, ग्रामीण पहुँच नीति, परिवर्तन व्यवस्थापन नीति, सूचना प्रविधि तालीम व्यवस्थापन नीति, तेश्रो पक्ष उपयोग नीति तयार गरेको हुनु पर्दछ । तर आशिकुडा सफ्टवेयरको सुरक्षा सम्बन्धमा सो अनुरुपका नीतिहरु तयार गरेका छैनन् । जसले गर्दा तथ्याङ्क तथा सफ्टवेयरको सुरक्षा सम्बन्धमा जोखिम हुने देखिन्छ ।

३.४ तेश्रोपक्ष आश्वस्तता तथा आन्तरीक लेखापरीक्षण : विभागले सञ्चालनमा रहेको सूचना प्रविधि प्रणालीको सूचना प्रविधि विभाग तथा स्वतन्त्र तेस्रो पक्षबाट सूचना प्रविधि लेखापरीक्षण गराउनु पर्दछ । विभागले प्रयोगमा ल्याएको आशिकुडावर्ल्ड सम्बन्धमा सूचना प्रविधि विभाग तथा स्वतन्त्र तेस्रो पक्षबाट उक्त प्रणाली परीक्षण गराएको छैन । जसले गर्दा आशिकुडावल्ड सम्बन्धमा भएमा जोखिमहरु विभागलाई पूर्व जानकारी नभई भविष्यमा सो समस्याको समाधानका लागि विभागलाई आवश्यक कदम पहल गर्न कठिन हुन्छ ।

३.५ जनशक्ति व्यवस्थापन : विभागमा प्रयोग भएको सफ्टवेयर सञ्चालन तथा व्यवस्थापनको लागि सूचना प्रविधि शाखामा निर्देशक-१, कम्प्यूटर अधिकृत-२ र कम्प्यूटर ईन्जिनियर-२ तथा अटोमेशन तथा विकास शाखामा निर्देशक-१, कम्प्यूटर अधिकृत-२ र कम्प्यूटर ईन्जिनियर-५ गरी जम्मा १३ जना कर्मचारीहरुको दरबन्दी रहेको छ । सूचना प्रविधि शाखामा २ कम्प्यूटर ईन्जिनियर र अटोमेशन तथा विकास शाखामा निर्देशक-१ र कम्प्यूटर इन्जिनियर-४ गरी ७ कर्मचारीहरुको पदपूर्ती भएको छैन । जसले गर्दा विभागको सूचना प्रविधि सम्बन्धि दैनिक सेवा प्रवाहमा असर पर्ने देखिन्छ ।

३.६ कर्मचारी तालिम : सूचना प्रविधिको तालीम सम्बन्धी योजना तयार गरी सूचना प्रविधि (आशिकुडा) प्रणाली संचालन गर्ने कर्मचारी तथा आवद्ध प्रयोगकर्ताहरुलाई सुरक्षा जागरण आवश्यक तालिम संचालन गरी प्रयोग

गर्न सक्षम तुल्याउनु पर्दछ । कर्मचारी तालिम सम्बन्धमा विभागमा संयुक्त राष्ट्रसघिय व्यापार तथा विकास सम्मेलन र विभागको आफ्नै तालिम योजना रहेको पाईयो । अंकटाडको तालिम सञ्चालन भएता पनि कर्मचारीको समय अभावले गर्दा विभागले आन्तरिक तालिम सञ्चालन गर्न नसकेको विभागको भनाई रहेको पाइयो । यसरी तालिम अभावले गर्दा कर्मचारीहरुलाई प्रणालीमा थप गरिएको नयाँ विशेषता उपर जानकारी हुदैँन । जसले गर्दा प्रणाली सञ्चालनमा कठिनाइ पर्न जान्छ ।

३.७हेल्पडेस्क : सूचना प्रविधि सफ्टवेयरको सञ्चालन सम्बन्धमा प्रयोगकर्ताहरुमा कुनै समस्या आएमा सोको जानकारी सफ्टवेयर सञ्चालन गर्ने केन्द्रलाई सफ्टवेयरको प्रणाली मार्फत जानकारी पठाउने तथा सोको अभिलेख राख्नको लागि सफ्टवेयरमा सहायता कक्षको व्यवस्था हुनुपर्दछ । तर यो सफ्टवेयरमा सहायता कक्षको व्यवस्था रहेको छैन । सफ्टवेयरको सञ्चालनमा प्रयोगकर्तालाई कुनै समस्या सृजना भएमा प्रयोगकर्ताहरुले सिधै भन्सार विभागका कर्मचारीहरुलाई फोन मार्फत गर्ने र सो पश्चात सुचना प्रविधि अधिकृतले गिट हव मार्फत समस्याको सम्बोधन गर्ने गरेको देखिन्छ । जसले गर्दा सफ्टवेयर सञ्चालनमा समस्या आउन सक्दछ ।

३.८ नियमितता परीक्षण : विभागमा प्रयोग गरिएको सूचना प्रविधि प्रणालीको सूरक्षा मापदण्ड तथा हार्डवेयर र सफ्टवेयर नियन्त्रणहरु ठीकसँग कार्यान्वयन भएको सुनिश्चत गर्नका लागि अपरेटिङ प्रणालीहरु अनुभवी सिस्टम ईन्जिनियर, सफ्टवेयर प्याकेजबाट परिक्षण, पेनेट्रेसन टेष्ट, सुरक्षा मापदण्ड र सन्चालन प्रणालीबाट नियमितताको जाँच गरिनु पर्दछ । तर आशिकुडा प्रणालीको सम्बन्धमा अहिलेसम्म सूचना प्रविधि विभागबाट पेनेट्रेसन टेष्ट नगराएको तथा कोबिट फाईभको अनुशरण गरेको छैन । साथै विभागले प्रणालीको नियमितता परिक्षणको लागि हालसम्म विशेष मापदण्ड मापदण्ड तयार गरेको छैन ।

३.९प्रक्रिया : विभागले प्रणाली सन्चालनका लागि, गोप्यिता र निष्ठता कायम गर्नको लागि औपचारिक प्रक्रिया स्थापित गरिएको हुनुपर्दछ । विभागद्धारा यस सम्बन्धमा उपयोगकर्ता दिग्दर्शन तयार गरेको भएता पनि सोको पुनरावलोकन गर्ने संयन्त्र रहेको पाईएन । जसले गर्दा संवेदनशील तथ्याङ्क तथा सूचनाहरुको खुलासा हुनसक्ने तथा प्रयोगकर्ताको अधिकार र दायित्वमा अस्पष्टता आउन सक्दछ ।

३.१० पासवर्ड : सफ्टवेयरको सूरक्षा सम्बन्धमा प्रणाली सन्चालक र साधारण प्रयोगकर्ताको लागि पासवर्ड नीति तथा प्रत्येक प्रयोगकर्ताको लागि अलग अलग युजर नेम र युजर आईडी हुनुपर्दछ । तर सफ्टवेयर प्रयोगकर्ता सम्बन्धमा पासवर्ड तथा पासवर्डकोको पालना तथा पासवर्ड नीति बनाएको छैन । जसले गर्दा सफ्टवेयरमा रहेको तथ्याङ्कको सुरक्षा नहुने तथा सफ्टवेयर सञ्चालनमा असर पर्न सक्दछ ।

३.११ उपयोगकर्ताको कार्य विभाजन : प्रणाली सञ्चालनको लागि प्रयोगकर्ता तथा प्रयोगकर्ताहरुको कामको स्पष्ट कार्य विवरण तयार गरिएको हुनुपर्दछ । प्रयोगकर्ताको अधिकार र दायित्व सम्बन्धमा स्पष्ट रुपमा कार्य विभाजन गरिएता पनि सोको पुनरावलोकन गर्ने गरिएको छैन । जसले गर्दा सफ्टवेयरको सञ्चालनमा समस्या आउन सक्दछ ।

३.१२ अडिट लग र अनुगमन : सफ्टवेयर सुरक्षाको लागि प्रणालीमा अडिट लगको व्यवस्था तथा त्यसको उचित अनुगमन गर्नु पर्दछ । आसिकुडा सफ्टवेयर सम्बन्धमा अडिट लगको व्यवस्था भएता पनि सोको अनुगमन एक निश्चित समयमा गर्ने नगरि सफ्टवेयर प्रयोगकर्तामा समस्या आए पश्चात मात्र सुपरीवेक्षण गर्ने गरिएको पाइयो । जसले गर्दा सफ्टवेयरको सुरक्षामा समस्या आउन सक्दछ ।

३.१३ नवप्रवेशी तथा छाडनेहरुको व्यवस्थापन(स्टार्टर एण्ड लिभर म्यानेजमेण्ट) : सफ्टवेयर सञ्चालनको लागि नयाँ प्रयोगकर्ता र पुरानो प्रयोगकर्ताको सरुवा सम्बन्धमा प्रोफाईल लक/चेञ्जको उचित व्यवस्था गरी नयाँ कर्मचारीको हकमा नयाँ उपयोगकर्ता आईडीको निर्माण तथा सरुवा भई जाने कर्मचारीको तत्काल युजर आईडी बन्द गर्ने व्यवस्था प्रणाली मार्फत नै गरिनु पर्दछ । तर यो सफ्टवेयर सञ्चालनको हकमा सो व्यवस्थाको परिपालना भएको पाईएन । जस्तैः नयाँ युजर आईडी सम्बन्धमा मिति २०७५ आश्विनमा भन्सार विभागबाट भैरहवा कार्यालय प्रमुख भई जानु भएका एक कर्मचारीले मिति २०७५ कार्तिक १४ मा मात्र फोन

मार्फत भन्सार विभागको सूचना प्रविधि शाखामा जानकारी गराएको पाईयो । जसले गर्दा सफ्टवेयरको सञ्चालनमा समस्या आउन सक्दछ ।

३.१४ एप्लिकेशन नियन्त्रण : विभागमा सञ्चालन भएको सफ्टवेयरको नियन्त्रणको लागि प्रणाली नक्शा (सिस्टम म्याप) तयार गरिएको हुनुपर्दछ । तर सफ्टवेयर सञ्चालन सम्बन्धमा प्रणाली नक्शा तयार गरेको छैन । जसले गर्दा सफ्टवेयरमा कुनै समस्या आई परेमा त्यसको समाधान गर्न कठिन हुन्छ ।

३.१५ एन्टिभाइरस : सूचना प्रविधि प्रणालीलाई हानी पुऱ्याउन सक्ने शंकास्पद तथा भाईरस युक्त कार्यक्रम(भाईरस/ म्यालिसियोस) ईत्यादिलाई नियन्त्रण गर्ने, पत्ता लगाउने र हटाउने एन्टि भाइरस प्रयोग गर्ने नीति तयार गरि कार्यान्वयन गरिनु पर्दछ । विभागले आशिकुडा सफ्टवेयरको सन्चालन प्रणाली(अपरेटिङ्ग सिस्टम) मा लिनक्सको प्रयोग गरिएकोले एन्टिभाइरसको आवश्यकता नपर्ने जानकारी दिएता पनि सो सम्बन्धी निर्णय अभिलेख गरेको देखिएन । सफ्टवेयरमा एन्टिभाईरस प्रयोग नगरिनुले अपलोड गरिएका फायलहरु स्क्यान नहुने, भाईरस आक्रमणबाट प्रणालीका तथ्यांक तथा सूचनाहरु काम नलाग्ने हुने तथा सफ्टवेयर सञ्चालनमा नै जोखिम रहन्छ ।

३.१६ डाटावेश सुरक्षा(डाटावेश सेक्युरिटि) : प्रणालीमा रहेका तथ्याङ्कहरुको सुरक्षाको निम्ति तथ्याङ्कआधारको सुरक्षाको व्यवस्था गरिएको हुनुपर्दछ । सफ्टवेयरको लागि तथ्याङ्क केन्द्रको व्यवस्था गरिएकोमा तथ्याङ्क आधार पढ्न नसक्ने (ईनक्रिपटेड) स्वरुपमा राखेको पाईएन ।

३.१७ पूर्वाधार सुरक्षा(फिजिकल सेक्युरिटी) : प्रणालीको तथ्याङ्क सुरक्षाको लागि उचित सुरक्षाको उपायहरु अवलम्बन गरिनु पर्दछ । यो प्रणालीको हकमा रेडियो फ्रिक्वेन्सी कार्ड तथा फिंगर थम्बको व्यवस्था गरिएको तथा बाहिरको मानिसलाई तथ्याङ्क केन्द्रमा प्रवेश गर्ने अनुमती नभएको तथा प्रवेश गरेमा आधिकारिक अधिकारीसँग प्रवेश गर्ने व्यवस्था रहेकोमा सो सम्बन्धमा भिजिटर लग रजिष्ट्रको व्यवस्था रहेको देखिएन । जसले गर्दा प्रणालीको तथ्याङ्क सुरक्षामा जोखिम आउन सक्दछ ।

३.१८ अनुगमन : विभागले स्वचालित कार्य सञ्चालनमा अनधिकृत फाइल, तथ्यांक वा गल्तिहरुलाई विश्लेषण गरि सफ्टवेयर तथा तथ्यांकहरुबाट हटाउन तथा रोक्नका लागि नियमित अनुगमन गरिनु पर्दछ । सूचना प्रविधिसँग सम्बन्धित कर्मचारीहरुले सन्दर्भ तथ्याङ्क(रिफरेन्स डाटा) जस्तैः साटफेर दर(एक्सतचेञ्ज डाटा) मात्र प्रणालीमा प्रविष्ट गर्दछन् । अन्य तथ्याङ्कहरु आयातकर्ता, निर्यातकर्ता तथा ब्रोकरले प्रविष्ट गर्दछन् । यदी प्रयोगकर्ताले अनाधिकृत तथ्याङ्क प्रणालीमा प्रविष्ट गरेमा यसलाई भन्सार अधिकृतद्धारा पुनरावलोकन, मूल्यांकन र सशोधन गरिन्छ । त्यसैले त्यहाँ अनाधिकृत अभिलेख तथा तथ्यांक नरहने सम्भावना रहेता पनि सफ्टवेयरमा त्यसलाई पुनरावलोकन गर्ने संयन्त्र रहेको पाईएन । यसले सामान्य व्यवसायिक कार्यसन्चालनमा ढिला हुने तथा प्रणाली समयानुकुल अद्यावधिक नहुने हुन्छ ।

३.१९ व्याकअप नीति : प्रणालीमा रहेका तथ्याङ्कहरुको सुरक्षाको निम्ति व्याकअप सृजना गरी त्यसको उचित परीक्षण गर्नु पर्दछ । विभागको आफ्नै डाटा सेन्टर मा प्रत्येक ५-५ मिनेटमा र राष्ट्रिय सूचना प्रविधि केन्द्रको डाटा सेन्टरमा प्रत्येक २-२ दिनमा व्याकअप दिईने भएता पनि डाटा व्याकअप को प्रक्रिया समुचित रुपमा सम्पन्न भए नभएको २-२ महिनामा परीक्षण गर्ने गरिएको भन्ने व्यवस्थापन पक्षबाट जानकारी गराएकोमा सोको अभिलेख राख्ने गरिएको छैन । जसले गर्दा डाटा व्याकअपको प्रक्रिया राम्रोसँग सम्पन्न भएको भनि विश्वस्त हुनसक्ने आधार नभई प्रणालीमा रहेको तथ्याङ्कको सुरक्षामा असर पर्न सक्दछ । अतः डाटा व्याकअपको प्रक्रिया राम्रोसँग सम्पन्न भए नभएको जाँच गर्नको लागि डाटा व्याकअप नीतिको तर्जुमा गरि सोको प्रभावकारीका साथ कार्यान्वयन गरी सोको अभिलेख राख्नु पर्दछ ।

३.२० ईन्टरफेस : विभागले नेटवर्क, डिस्क वा टेप्स मार्फत पुर्ण तथा शुद्ध तथ्याङ्कहरु स्थान्तरण गरेको र नेटवर्क मार्फत स्थान्तरण हुनेमा स्वचालित रुपमा गल्ति पत्तालगाउने र सुधार गर्ने सुविधा रहेको हुनु पर्दछ । परीक्षणको क्रममाः तथ्याङ्क स्थान्तरणको लागि कुनै पनि डिस्क, टेपको प्रयोग गरेको पाईएन । तथापि तथ्याङ्क स्थानान्तरण गर्नको लागि फाईबर च्यानल पोर्टकल र ट्रान्समिसन कन्ट्रोल प्रोटोकोलको प्रयोग गरेको पाईयो । तथ्याङ्क स्थान्तरणको क्रममाः देखापरेका समस्या र तथ्याङ्क स्थान्तरण पूर्ण रुपमा स्थान्तरण भए नभएको

त्यसको अभिलेख प्रत्येक ५-५ मिनेटमा गई बस्ने भएता पनि सोको पुनरावलोकन गर्ने संयन्त्र भने प्रणालीमा रहेको पाईएन । जसले गर्दा तथ्याङ्क स्थान्तरण गर्न प्रयोगमा ल्याईएको संयन्त्र माथि पूर्ण रुपमा विश्वस्त हुने स्थिति रहदैन ।

३.२१ वातावरणीय प्रतिरक्षा : सूचना प्रविधिमा प्रयोग हुने सम्पूर्ण हार्डवेयर तथा सफ्टवेयर आगलागी तथा बाढि पहिरोबाट नोक्सानी हुन नसक्ने वातावरणीय स्थानमा राखिएको र पुर्ण सुरक्षित विद्युतीय शक्ति तथा बैकल्पिक विद्युत आपूर्तीसमेतको व्यवस्था गरिएको हुनु पर्दछ । सूचना प्रविधि लेखापरीक्षणको क्रममा: विद्युत आपूर्तिको लागि नेपाल विद्युत प्राधिकरण मार्फत डेडिकेट लाईन तथा सिटी लाईन, ब्याट्री ब्याकअपकोलागि जेनेरेट्रर, आगलागी तथा बाढीको पूर्व जानकारी दिनको लागि अलआर्म तथा भुकम्प प्रतिरोधी भवनको समेट व्यवस्था रहेको छ । विभागले सम्पूर्ण हार्डवेयर तथा सफ्टवेयरहरुको आगलागी, बाढि, नियमित विद्युत आपुर्तीका लागी वैकल्पिक रुपमा राष्ट्रिय सुचना प्रविधि केन्द्रमा रहेको सरकारी सुचना डाटा केन्द्रमा व्यवस्था गरेता पनि सन्तोषजनक हुन सक्ने आधार नभएको विभागको भनाई रहेको पाईयो । यसबाट विभागको सूचना तथा तथ्याङ्क नोक्सानी हुनसक्ने जोखिम रहेको छ ।

३.२२ सेक्युरिटी लग्स् : सफ्टवेयर सुरक्षाको निम्ति सेक्युरिटी लग्स्को व्यवस्था गरि त्यसको समय समयमा मूल्यांकन तथा सुपरीवेक्षण गरिनु पर्दछ । सफ्टवेयरको सुरक्षाको निम्ति सेक्युरिटी लग्स्को व्यवस्थापन गरिएको भएता पनि विभागबाट सुपरीवेक्षण हुने गरेको छैन । जसले गर्दा सफ्टवेयर सञ्चालनमा असर पर्न सक्दछ ।

३.२३ सम्पत्ति अभिलेख : सुचना प्रविधिमा प्रयोग भाएका सबै हार्डवेयर तथा सफ्टवेयरको सम्पत्ति अभिलेख राख्ने र नियमित भौतिक परिक्षण गरि अभिलेख अद्यावधिक राखेको हुनु पर्दछ । विभागले हार्डवेयर तथा सफ्टवेयरको अभिलेख अन्य सम्पत्तिसंग राखेको र सो पनि स्पष्ट रहेको छैन । राष्ट्रिय सूचना तथ्याङ्क केन्द्रमा रहेको पूर्वाधारको मासिक रुपमा अवलोकन गर्ने गरको छ । विभागले सुचना प्रविधिसंग सम्बन्धित हार्डवेयर तथा सफ्टवेयरहरुको वर्गिकरण तथा व्यवस्थित सम्पत्ति अभिलेख राख्ने गरेको छैन र कुन कुन हार्डवेयर तथा सफ्टवेयर रहेको स्थानको अभिलेख ट्र्याकिङ्ग गर्ने गरेको पनि देखिएन । यसबाट सूचना प्रविधिका हार्डवेयर तथा सफ्टवेयर उपकरणहरुको प्रभावकारी उपयोगमा असर पर्नसक्छ ।

३.२४ तथ्याङ्क धुल्याउने : प्रणालीमा रहेको तथ्याङ्क धुल्याउनेसम्बन्धमा विभागद्धारा नीति तयार गरेको हुनुपर्दछ । आसिकुडा प्रणालीको हकमा तथ्याङ्क धुल्याउने नीति नबनाएको र सूचना प्रविधि लेखापरीक्षण भएको दिनसम्म विभागबाट कुनै पनि तथ्याङ्क धुल्याउने गराएको छैन । जसले गर्दा तथ्याङ्क भण्डारण अनावश्यक तथा पुराना तथ्याङ्कहरुले भरिन गई सूचना प्रविधि प्रणालीको सञ्चालनमा असर पर्न सक्दछ ।

३.२५ व्यवसाय निरन्तरता योजना र प्रकोप पुनःस्थापना योजना (बी.सी.पी तथा डि.आर.पी) : सफ्टवेयरको सुरक्षा तथा व्यवसायिक निरन्तरताको लागि विभागद्धारा व्यवसायिक निरन्तर योजना तथा प्रकोप पुनःस्थापन योजना निर्माण गरी कार्यान्वयनमा ल्याउनु पर्नेमा विभागबाट सो अनुसारको काम भएको छैन । जसले गर्दा सफ्टवेयर सञ्चालनमा असर पर्न सक्दछ ।

३.२६ सफ्टवेयरको अभिलेखिकरण : नेपाल सरकारको सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१ को दफा ४ अनुसार नेपाल सरकारका निकायहरुमा प्रयोगमा रहेका सूचना प्रविधि प्रणालीलाई वर्गीकरण गर्ने प्रयोजनार्थ सूचना प्रविधि विभागमा अभिलेखिकरण गराउनु पर्ने व्यवस्था छ । तर भन्सार विभागबाट उपयोगमा ल्याईएका आसिँकुडा लगायतका सफ्टवेयरहरु सूचना प्रविधि विभागमा अभिलेखीकरण गराएको छैन । जसले गर्दा सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिकाले गरेको व्यवस्थाको परिपालना हुन सकेको छैन ।

३.२७ अनुकुलित/परिमार्जीत आई टी प्रणाली(कस्टुमाईज्ड/बीस्कोप आइटी सिस्टम) : विभागले सूचना प्रविधि प्रणालीलाई विभागको कामको रणनीति, परिभाषित आवश्यकता तथा मापदण्ड, जोखिम विश्लेषण, लागत -लाभ विश्लेषण, सुरक्षा जोखिम मूल्याङ्कन(सेक्यूरिटी रिस्क म्यानेजमेण्ट) अनुसार प्रणाली विकास, परिमार्जन तथा सुधार गर्ने गरि प्राथमिकता निर्धारण गरिनु पर्दछ । विभागले अहिले प्रयोग गरिरहेको

सफ्टवेयर अनुकुलित सफ्टवेयर रहेको र व्यवसायको आवश्यकता अनुसार सफ्टवेयरलाई अनुकुलित गरिएको तथा केन्द्रिकृत सफ्टवेयर भएको कारणले गर्दा नै विभागले यसलाई अनुकुलित गर्ने गरेको भनाई रहेको छ ।

३.२८ कार्य विभाजन : विभागले सफ्टवेयर प्रणालीको तथ्याङ्कहरुको विकास, परिमार्जन, परिक्षण, कार्यान्वयन र स्थान्तरण गर्ने कार्य फरक फरक बातावरणमा व्यवस्थित गरेको हुनुपर्दछ । विभागमा प्रणालीको छुट्टा छुट्टै परिक्षण(टेस्टं) तथा लाईभ ईनभ्यारेमेण्ट गर्ने गरेको साथै प्रणाली निमार्णकर्ताले टेस्ट सर्भरमा सफ्टवेयरको परिक्षण तथा स्वीकृत गरी अन्य सूचना प्रविधिसँग सम्बन्धित कर्मचारीहरुले यसलाई प्रयोगमा ल्याउने गरेको छ । तर सफट्वेयर निर्माणकर्ता र सफ्टवेयर जाँचकर्ता एउटै रहेको छ । जसले गर्दा सफ्टवेयर निर्माणकर्ता र परिक्षणकर्ता एउटै व्यक्ति हुदाँ सफ्टवेयरको गुणस्तरमा आश्वस्तता हुन सक्ने स्थति रहदैँन । अत: विभागले यसतर्फ उचित ध्यान पुऱ्याउनु पर्ने देखिन्छ ।

३.२९ उपयोगककर्ता स्वीकृती परिक्षण(यूजर ऐसेप्टेन्स टेस्ट) : विभागले विकास तथा परिमार्जन गरेको सफ्टवेयर प्रणालीलाई प्रयोगमा लैजानु भन्दा पहिला लाभग्राहीहरुलाई उपयोगमा सहज हुने वा समस्या नआउने सम्बन्धमा उपयोगकर्ता स्वीकृति परिक्षण गराउनु पर्दछ । विभागले आशिकुडा प्रणालीको उपयोगकर्ता स्वीकृति परिक्षण गराएको छैन । जसले गर्दा सफ्टवेयरले वास्तविक रुपमा आफ्नो उद्देश्य हासिल गर्न नसक्ने जोखिम रहन्छ

३.३० वारेण्टी : विभागले प्राप्ति गरेका हार्डवेयर तथा सफ्टवेयरको वारेण्टीको सम्झौता(वारेण्टी एग्रिमेण्ट) समेत गरेको हुनु पर्दछ । विभागले हार्डवेयर तथा सफ्टवेयर खरिद गर्दा सोको स्पेसिफिकेशनमा वारेन्टि हुने जनाएतापनि विभागले वारेन्टिसम्बन्धि अभिलेखहरु राखेको छैन । यसबाट हार्डवेयर तथा सफ्टवेयरको उपयोग अवधिको सुनिश्चितता तथा सन्चालन/मर्मत लागत बृद्धिको जोखिम बढेको छ ।

३.३१ प्रयोग पश्चात पुनरावलोकन(पोस्ट इम्प्लीमेन्टेसन रिभ्यू) : विभागमा प्रयोगमा आएको सफ्टवेयर प्रणालीको विकास तथा परिमार्जन सम्बन्धमा कार्यसम्पादनको निश्चित समयमा प्रयोग पश्चात पुनरावलोकन गरिएको हुनु पर्दछ । विभागले आशिकुडाको कार्यान्वयन पछीको पुनरावलोकन ७ जुलाई, २०१७ मा एडीबीद्वारा गराइएको छ । उक्त प्रतिवेदनमा आशिकुडाप्रणालीको प्रभावकारी सञ्चालनको लागि कार्यगत कार्यान्वयन र प्राविधिक कार्यान्वयन सम्बन्धमा समय सीमा सहित सुझावहरु उल्लेख गरिएको छ । विभागले सूचना प्रविधि लेखापरीक्षणको समय सम्म उक्त सुझावहरुको कार्यान्वयन गरेको छैन । जसले गर्दा आशिकुडा प्रणालीको सञ्चालनमा समस्या आउन सक्ने जोखिम रहन्छ ।

३.३२ भन्सार महसुल दर परिवर्तन : सूचना प्रविधि प्रणालीमा प्रत्येक बजेट भाषण पछि भन्सार महसुल दरमा भएको परिवर्तन गर्न प्रणाली स्थापना गरेको हुनु पर्छ । भन्सार दर बजेट भाषण संगै दरहरू परिवर्तन गरीएता पनि पुनरावलोकन गरीएको छैन । यसले गर्दा भन्सार दरमा असर पर्न जान्छ ।

३.३३ समूह गठन : सूचना प्रविधि प्रणालीमा भन्सार दरहरू परिवर्तन गर्न एडमिन यूजर टिम हुनुपर्छ । तर भन्सार विभागमा भन्सार दर परिवर्तन लागू गर्न टोली गठन गरेको जनाएता पनि त्यसको अभिलेख राखेको पाइएन । यसले गर्दा अनधिकृत सदस्यहरूले प्रणालीमा दर परिवर्तन र अपडेट गर्न सक्दछ ।

३.३४ मूल्य अभिवृद्धि कर : भन्सार एजेन्टले गल्ति र जालसाजिपूर्ण सूचना प्रविष्टि गरेको खण्डमा सोको चेक र नियन्त्रण गर्ने प्रणाली हुनुपर्छ । तर सहुलियत प्राप्त गर्ने उद्देश्यले कमर्सियल ईनभ्वाईसलाई नै सहुलियत प्रमाणको रुपमा अपलोड गरि भन्सार तथा मूल्य अभिबृद्धि कर छुट दिएको देखियो । केही नमुनाहरुको परीक्षण गर्दा वीरगन्जस्थित सुख्खा बन्दरगाह भन्सारका एक एजेन्टले कागजात प्रविष्टि गर्दा गलत प्रमाण अपलोड गरी सोही कागजात भन्सार अधिकृतले स्वीकृत गरी भन्सार जांचपास गरेको देखियो । यसले गर्दा राजस्व छली हुन सक्ने देखियो । छनौट गरिएका नमुनाहरु देहाय अनुसार छन् ।

पीपी नं.	एजेण्ट नं.	मिति	लेन सेलेक्टीभिटी	कैफियत
एम १०७४३	२७०	१९-०६-२०१८	रातो	व्यवपारिक वील लाई भन्सार महशुल तथा
एम १२८३२	२७०	२५-०७-२०१८	रातो	

एम १३९८०	२७०	१४-०८-२०१८	रातो	मूल्य अभिवृद्धि कर छुट सुविधा पाउने प्रमाणको रुपमा पुनः अपलोड गरेको
एम ८२९२	२७०	१०-०५-२०१८	रातो	
एम १५२९७	२७०	०६-०९-२०१८	रातो	
एम ५२७८	२७०	२२-०३-२०१८	रातो	
एम ८३३९	२७०	११-१५-२०१८	रातो	
एम ८२९२	२७०	१०-०५-२०१८	रातो	

३.३५ बैंक जमानतको अनुगमन : बैंक ग्यारेन्टीको नियन्त्रण र निरीक्षणका लागि आशिकुडा सफ्टववेयर संयन्त्रमा व्यवस्था गरेको हुनुपर्छ । नेपाल भन्सार जाँचपास प्रणालीको सफ्टवेयर सुचना प्रविधि प्रणालीमा बैंक जमानतलाई स्वत प्रमाणित तथा अनुगमन गर्न कुनै व्यवस्था रहेको छैन । उक्त बैक जमानतको समय सकिएको र नक्कली वैक ग्यारेन्टी समेतवाट कारोबार हुन सक्ने देखियो । सोको जानकारी यस प्रणालीवाट पाउन नसकिदा राजस्व गुम्न सक्ने देखिन्छ ।

परिच्छेद-४ : सुझाव

४.१ लेखापरीक्षणबाट देखिएका उल्लिखत ब्यहोराहरुका सम्बन्धमा निम्न अनुसारका सुझाव कार्यान्वयन गर्नु उपयुक्त देखिन्छ :

४.२ सूचना प्रविधि निर्देशक समिति : सूचना प्रविधि सम्बन्धमा देखिएका नविन अवधारणा तथा आन्तरिक रुपमा देखिएका समस्या तथा चुनौती उपर निर्णय लिनको लागि विभागमा सूचना प्रविधि निर्देशक समिति गठन गरेता हालसम्म कुनैपनि काम नगरेकोले उक्त समितिलाई कार्यान्वयनमा ल्याईनु पर्दछ ।

४.३ वार्षिक तथा रणनैतिक योजना : विभागले स्वचालित भन्सार जाँचपास प्रणाली (आशिकुडा) सम्बन्धमा वार्षिक रुपमा गरिने कार्यको लागि वार्षिक तथा रणनैतिक योजना तयार गरी कार्यान्वयन गर्नु पर्दछ ।

४.४ सूचना प्रविधि नीति : विभागमा प्रयोग भएको सफ्टवेयर सुरक्षाको लागि विभागले निम्नानुसारको नीतिहरु तर्जुमा गरी कार्यान्वयनमा ल्याईनु पर्दछ : सूरक्षा नीति, व्यवसाय निरन्तरता नीति, डिजास्टर रिकभरी नीति, हार्डवेयर नीति, सफ्टवेयर नीति, तथ्याङ्कहरुको गोपनियता नीति, व्याकअप नीति, परिवर्तन व्यवस्थापन नीति, दूर पहुँच नीति, सूचना प्रविधि तालीम व्यवस्थापन नीति ,तेश्रो पक्ष उपयोग नीति, लग ईन/लग आउट नीति, फायरवाल नीति ।

४.५ तेश्रोपक्ष आश्वस्तता तथा आन्तरीक लेखापरीक्षण : विभागले प्रयोगमा ल्याएको सूचना प्रविधि प्रणालीको सूचना प्रविधि विभाग तथा तेश्रोपक्ष मार्फत सूचना प्रविधि लेखापरीक्षण गराईनु पर्दछ ।

४.६ जनशक्ति व्यवस्थापन : विभागमा प्रयोग भएको सफ्टवेयर सञ्चालन तथा व्यवस्थापनको लागि सूचना प्रविधि शाखामा दरबन्दी अनुसार सूचना प्रविधि जनशक्तिको पदपूर्ती गरिनु पर्दछ ।

४.७ कर्मचारी तालीम : सूचना प्रविधि प्रणालीमा आएका नवीन अवधारणा तथा विशेषताहरुलाई आत्मसात गर्नको लागि विभागले वार्षिक कार्यक्रममा तालिम स्वीकृत गराई सो अनुसारको तालिम सञ्चालन गरिनु पर्दछ ।

४.८ हेल्पडेस्क : सूचना प्रविधि सफ्टवेयरको सञ्चालन सम्बन्धमा प्रयोगकर्ताहरुमा कुनै समस्या आएमा सोको जानकारी सफ्टवेयर सञ्चालन गर्ने केन्द्रलाई सफ्टवेयरको प्रणाली मार्फत जानकारी पठाउने तथा सोको अभिलेख राख्नको लागि सफ्टवेयरमा सहायता कक्षको व्यवस्था गरिनु पर्दछ ।

४.९ नियमितता परिक्षण : विभागले सूचना प्रविधि प्रणालीको नियमितता परीक्षणको लागि विशेषिकृत मापदण्ड तयार गर्नुपर्ने तथा सूचना प्रविधि विभागबाट पेनेट्रेसन टेष्ट गराईनु पर्दछ ।

4.1.10 **प्रक्रिया :** विभागले सफ्टवेयर सञ्चालन सम्बन्धमा उपयोगकर्ता दिग्दर्शन तयार गरी सोको पुनरावलोकन गर्ने संयन्त्रको विकास गरिनु पर्दछ ।

4.1.11 **पासवर्ड :** विभागले प्रत्येक प्रयोगकर्ताको लागि अलग अलग युजर नेम, युजर आईडि, पासवर्ड क्यारेक्टर(अल्फा, न्यूमेरिक, स्यामबोल) तथा पासवर्डको न्यूनतम क्यारेक्टर र अधिकतम क्यारेक्टरको व्यवस्था तथा पासवर्ड नीतिको उचित व्यवस्था गरिनु पर्दछ ।

4.1.12 **उपयोगकर्ताको कार्य विभाजन :** विभागले प्रणाली सञ्चालन सम्बन्धमा प्रयोगकर्ताको लागि तयार गरिएको कामको स्पष्ट विवरणको समय समयमा पुनरावलोकन गर्ने संयन्त्र तयार गरि सोको सुपरीवेक्षण गरिनु पर्दछ ।

4.1.13 **अडिट लग र अनुगमन** : विभागले सूचना प्रविधि प्रणालीको सुरक्षाको लागि प्रणालीमा कुनै समस्या सृजना हुनुपूर्व नै अडिट लगको निश्चित समय समयमा उचित अनुगमन गर्ने संयन्त्रको विकास गरिनु पर्दछ ।

4.1.14 **नवप्रवेशी तथा छाडनेहरुको व्यवस्थापन(स्टार्टर एण्ड लिभर म्यानेजमेण्ट) :** विभागले सरुवा भई आउने तथा सरुवा भई जाने सफ्टवेयर प्रयोगकर्ताको युजर आईडिको निर्माण र प्रोफाईल लक गर्दा प्रणाली मार्फत नै गरिने संयन्त्रको विकास गरिनु पर्दछ ।

4.1.15 **एप्लिकेशन नियन्त्रण :** विभागले सञ्चालनमा ल्याएको सूचना प्रविधि प्रणाली सम्बन्धमा स्पष्ट प्रणाली नक्शा बनाई कार्यान्वयनमा ल्याईनु पर्दछ ।

4.1.16 **एन्टिभाइरस** : विभागले आशिकुडा सफ्टवेयर प्रणालीमा अपलोड हुने अभिलेख तथा फायलहरु स्वतः स्क्यान हुने एन्टिभाइरस सफ्टवेयर जडान गरि आशिकुडा प्रणालीलाई सुरक्षित राखिनु पर्दछ ।

4.1.17 **डाटावेश सुरक्षा(डाटावेश सेक्यूरिटि) :** विभागले तथ्याङ्क केन्द्र राखेको तथ्याङ्कको सुरक्षाको निम्ति तथ्याङ्कलाई ईनक्रिपटेड स्वरुपमा राख्ने संयन्त्रको विकास गरिनु पर्दछ ।

4.1.18 **पूर्वाधार सुरक्षा(फिजिकल सेक्यूरिटी)** : बाहिरबाट विभागको तथ्याङ्क केन्द्रमा प्रवेश गर्ने आगन्तुकहरुको लागि भिजिटर लग रजिष्ट्ररको व्यवस्था गरिनु पर्दछ ।

4.1.19 **अनुगमन :** सूचना प्रविधि प्रणालीमा प्रविष्ट हुने अनधिकृत फाइल, तथ्यांक वा गल्तिहरुलाई विश्लेषण गरि सफ्टवेयर तथा तथ्यांकहरुबाट हटाउन तथा रोक्नका लागि विभागबाट नियमित अनुगमन एंव पुनरावलोकन गरिनु पर्दछ ।

4.1.20 **व्याकअप नीति :** डाटा व्याकअपको प्रक्रिया राम्रोसँग सम्पन्न भए नभएको जाँच गर्नको लागि डाटा व्याकअप नीतिको तर्जुमा गरि सोको प्रभावकारीका साथ कार्यान्वयन गरिनु पर्दछ ।

4.1.21 **ईन्टरफेस :** तथ्याङ्क स्थानन्तरण गर्न प्रयोगमा ल्याईका संयन्त्रहरु ट्रान्समिसन कन्ट्रोल प्रोटोकल र फाईबर च्यानल पोर्टकलको निश्चित समयावधिमा पुनरवलोकन गर्ने संयन्त्रको विकास गरिनु पर्दछ ।

4.1.22 **वातावरणीय प्रतिरक्षा :** सरकारी एकीकृत डाटा सेन्टरमा रहेको सूचना तथा तथ्याङ्कहरु सुरक्षित राख्नको लागि सूचना तथा तथ्याङ्कहरु सुरक्षित हुने आस्वश्तता सहितको पूर्वाधार तथा संयन्त्रको विकास गरिनु पर्दछ ।

4.1.23 **सेक्युरिटी लग्स् :** सफ्टवेयरको सुरक्षाको निम्ति प्रयोग गरिएको सेक्युरिटी लग्स्को समय समयमा सुपरीवेक्षण गरी सुपरीवेक्षण गरिएको अभिलेख तयार गरिनु पर्दछ ।

4.1.24 **सम्पत्ति अभिलेख :** सूचना प्रविधिमा प्रयोग भएका हार्डवेयर तथा सफ्वेयरको प्राप्ति मिति, वारेण्टि अवधि, उपयोग मिति तथा स्वामित्वको अवस्था देखिने विस्तृत विवरणसहितको अभिलेख राखिनु पर्दछ ।

4.1.25 **तथ्याङ्क धुल्याउने :** सूचना प्रविधि प्रणालीमा रहेको तथ्याङ्कको सुरक्षाको लागि तथ्याङ्क धुल्याउने नीतिको तर्जुमा गरी समयानुसार तथ्याङ्कको वर्गिकरण पश्चात पूराना तथा महत्वहिन तथ्याङ्कहरुलाई नष्ट गरिनु पर्दछ ।

4.1.26 **व्यवसाय निरन्तरता योजना र प्रकोप पुनःस्थापना योजना (बी.सी.पी तथा डि.आर.पी) :** विभागले व्यावसायिक योजना तथा प्रकोप पुनः स्थापना योजनाको निर्माण गरी कार्यान्वयनमा ल्याईनु पर्दछ ।

4.1.27 **सफ्टवेयरको अभिलेखिकरण** : नेपाल सरकारको सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका ,२०७१ मा भएको व्यवस्थाको परिपालना गरी उपयोगमा ल्याईएको सफ्टवेयरहरु सूचना प्रविधि विभागमा अभिलेखिकरण गरिनु पर्दछ ।

4.1.28 **अनुकुलित/परिमार्जीत आई टी प्रणाली(कस्टुमाईज्ड/बीस्कोप आइटी सिस्टम) :** विभागको आवश्यकता अनुसार अनुकुलित तथा परिमार्जित आई टी प्रणाली मध्ये कुन उपयुक्त हुने हो परिक्षण गरी सो अनुसारको आई टी प्रणाली प्रयोगमा ल्याईनु पर्दछ ।

4.1.29 **कार्य विभाजन :** सफ्टवेयरको गुणस्तर आश्वस्तताको लागि सफ्टवेयरको निर्माणकर्ता तथा सफ्टवेयरको जाँचकर्ता फरक हुने गरी सूचना प्रविधि प्रणालीको छुट्टा छुट्टै परीक्षण तथा लाईभ ईनभ्यारेमेण्ट परीक्षण गरिनु पर्दछ ।

4.1.30 **उपयोगककर्ता स्वीकृती परिक्षण(यूजर ऐसेपटेन्स टेस्ट) :** सफ्टवेयरलाई प्रयोगमा ल्याउनु पूर्व उपयोगकर्ता स्वीकृति परिक्षण(यूजर एसप्टेन्स टेस्ट) पश्चातमात्र उपयोगमा ल्याउने गरिनु पर्दछ ।

4.1.31 **वारेण्टी :** हार्डवेयर तथा सफ्टवेयर प्राप्ति गर्दा निश्चित अवधिको वारेन्टि सहित लागत लाभ विश्लेषण गरिएको हुनु पर्दछ ।

4.1.32 **प्रयोग पश्चात पुनरावलोकन(पोस्ट इम्प्लीमेन्टेसन रिभ्यू) :** ए.डि.बि.द्धारा आशिकुडाप्रणालीको पुनरावलोकन पश्चात दिईएका सुझावहरु विभागद्धारा कार्यान्वयन गरिनु पर्दछ ।

4.1.33 **भन्सार महसुल दर परिवर्तन** : भन्सार दर बजेट भाषण संगै दरहरू परिवर्तन गरिएपछि सोको समय समयमा पुनरावलोकन गरिनु पर्दछ ।

4.1.34 **समूह गठन** : भन्सार दर परिवर्तन लागू गर्न एडमिन यूजर टिम गरिएको टोलीले गरेका कामहरुको अभिलेख राख्नु पर्दछ ।

4.1.35 **मूल्य अभिवृद्धि कर छलीको सम्भावना** : भन्सार एजेन्टले प्रविष्टि गरेको सूचना नमूनाको आधारमा छनौट गरी विश्लेषण गर्दा सहुलीयत प्राप्त गर्ने उद्देश्यले कमरसियल ईनभ्वाईसलाई नै सहुलियत प्रमाणको रुपमा अपलोड गरि भन्सार तथा मुल्य अभिवृद्धि कर छुट दिएको देखिएकोले यस सम्बन्धमा विस्तृत छानविन गरि गलत कागजात अपलोड गर्ने भन्सार एजेन्ट तथा कर्मचारीलाई कारवाही गरि घटि महशुल असुल गरिनु पर्ने देखिन्छ ।

4.1.36 **बैंक जमानतको अनुगमन** : स्वचालित भन्सार जाँचपास प्रणालीले स्वचालित रुपमा बैंक जमानतको परीक्षण तथा अनुगमन गर्ने संयन्त्रको विकास गरिनु पर्दछ ।

४.२ निष्कर्ष :

भन्सार जाँचपास प्रणालीलाई सूचना प्रविधिमा आधारित बनाउने उद्देश्यले सन् १९९६ देखि स्वचालित भन्सार जाँचपास प्रणालीलाई प्रयोगमा ल्याईएता पनि विभागले प्रयोगमा ल्याएको आशिकुडा सूचना प्रविधि प्रणालीको सुरक्षा सम्बन्धमा हालसम्म सूचना प्रविधि नीति, सूरक्षा नीति, व्यवसाय निरन्तरता नीति, डिजास्टर रिकभरी नीति लगायतका नीतिहरु तयार नगरेको, सूचना प्रविधि विभाग तथा तेश्रोपक्ष मार्फत सूचना प्रविधि लेखापरीक्षण नगराएको तथा भि.ए.पि.टी. टेस्ट नगराएको, सेक्युरिटी लग्सको समय समयमा सुपरीवेक्षण हुने नगरेको, प्रयोगमा ल्याएको सूचना प्रविधि प्रणालीहरु सूचना प्रविधि विभागमा अभिलेखिकरण नगरिएको, सूचना प्रविधि प्रणाली प्रयोगमा ल्याउनु पूर्व यूजर एसप्टेन्स टेस्ट नगराएको जस्ता व्यहोराहरु देखिएकोमा आशिकुडा प्रणालीको उद्देश्य प्राप्ति तथा भन्सार जाँचपास प्रणालीलाई पूर्णत सूचना प्रविधिमा आधारित बनाउनको लागि उल्लेखित सुधारका उपायहरुलाई अवलम्बन गरिनु पर्दछ ।