विद्युतीय सरकारी खरिद(ई-जिपी) को उपयोग स्थिति मूल्यांकन

परिच्छेद-१ : पृष्ठभूमि

१.१ **स्थापना, उद्देश्य र कार्यक्षेत्र :** सार्वजनिक खारिद ऐन, २०६३ तथा नियमावली, २०६४ ले व्यवस्था गरेका विधि र प्रक्रिया विधिसम्मत तरिकाले लागु भए नभएको सन्दर्भमा अनुगमन गरी लागु गराउने महत्वपूर्ण निकायको रुपमा सार्वजनिक खरिद अनुगमन कार्यालयको मिति २०६४।५।३ मा स्थापना भएको हो । सार्वजनिक खरिद अनुगमन कार्यालयले सार्वजनिक खरिद प्रक्रियामा देखिएको अस्वस्थ प्रतिस्पर्धालाई न्यून गरी खरिद प्रक्रियालाई खुल्ला, पारदर्शी, वस्तुनिष्ठ र विश्वसनीय बनाउने उद्देश्यले सिंगल पोर्टलमा आधारित सार्वजनिक विद्युतीय खरिद प्रणाली प्रणालीको विकास भएको हो । त्यो प्रणालीमा अनलाईन मूल्याँकन, ठेक्का सम्झौता, ठेक्का व्यवस्थापन, विद्युतीय भुक्तानी लगायतका प्रणालीहरु थप गरी सम्पूर्ण खरिद प्रणालीलाई व्यवस्थित, वैज्ञानिक र तथ्याङ्कीय सुरक्षा सहितको सार्वजनिक खरिद व्यवस्थापन सूचना प्रणालीमा आवद्ध गरी विद्युतीय बोलपत्र सम्बन्धी सम्पूर्ण कामहरु यसै प्रणाली हुने गर्दछ । सार्वजनिक खरिद ऐन, २०६३ को दफा १४(२) अनुसार बोलपत्रको सूचना सर्वजनिक खरिद अनुगमन कार्यालय र सम्बन्धित निकायको वेव साईटमा राख्नुपर्ने र नियमावलीको नियम १४६ अनुसार निकायहरुको विद्युतीय खरिद प्रणालीको पोर्टेलमा दर्ता भई खरिद कारवाही सञ्चालन गर्नुपर्ने व्यवस्था रहेको छ । यस प्रणालीको कार्यक्षेत्र राज्यका सरकारी तथा सार्वजनिक कार्यालयहरुको वस्तु तथा सेवा खरिद सम्बन्धी बोलपत्र सूचना प्रकाशन देखि मूल्यांकन तथा आसय पत्रको सूचना जारीसम्म रहेको छ ।

१.२ **कानूनी व्यवस्था :** सार्वजनिक खरिद ऐन, २०६३ तथा नियमावली, २०६४, विद्युतीय कारोबार ऐन,२०६३ तथा नियमावली, २०६४

१.३ **नीतिगत व्यवस्था :** सरकारी निकायको वेव साईट निर्माण तथा व्यवस्थापन सम्बन्धि निर्देशिका, २०६८, सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१, सूचना तथा सञ्चार प्रविधि नीति, २०७२, विद्युतिय खरिद प्रणाली सञ्चालन मार्गनिर्देशिका, २०७३ (प्राविधिक मार्गदर्शन), विद्युतिय खरिद प्रणाली सञ्चालन निर्देशिका, २०७४, राष्ट्रिय विद्युतीय शासन गुरुयोजना, नेपाल जीइए इन्फ्रास्ट्रक्चर आर्किटेक्चर, सूचना तथा सञ्चार प्रविधि नीति, २०७४, सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका ।

१.४ चालु वर्षको वजेट वक्तव्यमा उल्लेख भएका प्रमुख व्यवस्था :

- सूचना तथा सञ्चार प्रविधिका लागि 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 स्थपना 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 मूल्यांकनका लागि 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 पूवांधार ,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 परिपालना को जाँच गर्नु पनि यस लेखापरीक्षणको उद्देश्य रहेको छ ।

२.२ **लेखापरीक्षणको क्षेत्र** : यस लेखापरीक्षणले सार्वजनिक खरिद अनुगमन कार्यालय र विद्युतीय खरिद प्रक्रिया अवलम्बन गर्ने सरकारी निकायहरुको सूचना प्रविधि संयन्त्र र विशेष गरी यस कार्यालयहरुमा प्रयोगमा ल्याईएका 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 जनशक्ति, कार्यालय प्रमुख र अन्य पदाधिकारीसँगको छलफल र तथ्याङ्क परीक्षण तथा विश्लेषण गरिएको छ ।

२.४ **सीमा** : यो लेखापरीक्षणमा नमुना छनौट, मानवीय त्रुटि, कारोबार र प्रणालीको जटिलता एंव अनिश्चतता, समयको कमी, समयमै सूचना प्राप्त नहुने, ईत्यादि सीमितताका रुपमा रहेका छन् ।

परिच्छेद-३ : लेखापरीक्षणवाट देखिएका व्यहोराहरु :

३.१ **सूचना प्रविधि निर्देशक समिति :** सूचना प्रविधि सम्बन्धमा देखिएका नविन अवधारणा तथा आन्तरिक रुपमा देखिएका समस्या तथा चुनौती उपर निर्णय लिनकोलागि कार्यालयमा सूचना प्रविधि निर्देशक समिति गठन गरिनु पर्दछ । सार्वजनिक खरिद अनुगमन कार्यालयमा स्टेरिङ्ग कमिटी गठन भएको देखिएन । जसले गर्दा सूचना प्रविधिमा असहज भई सूचना प्रविधि कार्यमा रोकावट आउन सक्दछ ।

३.२ **वार्षिक तथा रणनैतिक योजना** : कार्यालयले सूचना प्रविधि सम्बन्धमा रणनैतिक योजना तथा वार्षिक योजना तयार गरेको हुनुपर्दछ । सार्वजनिक खरिद अनुगमन कार्यालयले सूचना प्रविधि सम्बन्धि रणनैनिक तथा वार्षिक योजनाहरु तयार गरेको देखिएन । जसले गर्दा कार्यालयमा सूचना प्रविधिको निरन्तरता तथा सूचना प्रविधि विकासमा सहजता आउन सक्दैँन ।

३.३ **सूचना प्रविधि नीति** : कार्यालयमा 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 ई-जिपी सफ्टवेयरको सूरक्षा सम्बन्धमा सो अनुरुपका नीतिहरु तयार गरेका छैनन् । जसले गर्दा तथ्याङ्क तथा सफ्टवेयरको सुरक्षा सम्बन्धमा जोखिम हुने देखिन्छ ।

३.४ **तेश्रोपक्ष आश्वस्तता :** कार्यालयले प्रयोग गरेको विद्युतीय खरिद प्रणाली(ई-जिपी) लगायत सूचना प्रविधिको प्रक्रिया, उपयोग, सन्चालन, व्यवस्थापन तथा अनुगमनकालागी स्वतन्त्र एवं निश्पक्ष सूचना प्रविधि विशेषज्ञबाट आश्वस्तता परिक्षण गराएको हुनु पर्दछ । कार्यालयले विश्व बैकको आर्थिक सहयोगमा नियुक्त तेश्रोपक्ष डिलोइट टच तोमात्सु इण्डिया एलएलपी कम्पनीबाट सूचना प्रविधि प्रणालीको आश्वस्तता परीक्षण गराएको देखियो । उक्त कम्पनिले २४ अप्रिल २०१८ मा पेश गरेको प्रतिवेदनमा विभिन्न सुधारका कार्यक्रम कार्यान्वयन गर्न सुझाउ दिएकोमा कार्यालयबाट सो मध्ये सूचना प्रविधि प्रणाली सुधार गर्नुपर्ने सूचना प्रविधि नीति तयार गर्नुपर्ने, अभिलेख व्यवस्थित गर्नुपर्ने, नेटवर्क व्यवस्थापन टुल्स (नागिओस) अपग्रेड गर्नुपर्ने लगायत ३८ वटा सुझाउ कार्यान्वयन गरेको छैन भने इनएक्टिभ यूजरलाई १२ महिना पछि स्वतः डिसएवल गर्नुपर्ने, प्रणाली सन्चालनमा अधिकार र जिम्मेवारीको कार्यविवरण बनाउने समेत विभिन्न ५ वटा सुझाउहरु आँसिक कार्यान्वयन गरेको विवरण दिएको छ । जसले गर्दा ई-जिपी प्रणालीको सञ्चालनमा समस्या आउन सक्ने जोखिम रहन्छ ।

३.५ **आन्तरीक लेखापरीक्षण** : कार्यालयले प्रयोग गरेको सूचना प्रविधिका सफ्टवेयरको आन्तरीक लेखापरीक्षण गराएको हुनु पर्दछ । कार्यालयका अनुसार कर्मचारी अभावले आन्तरीक लेखापरीक्षण शाखा गठन गरेको छैन । जसले गर्दा प्रणालीमा देखापरेका समस्याहरुको पूर्व ज्ञान नभई सूचना प्रविधि प्रणाली सञ्चालनमा कठिनाई सृजना हुन सक्दछ ।

३.६ **जनशक्ति व्यवस्थापन** : सूचना प्रविधि व्यवस्थापन गर्न कार्य विवरण तथा कार्यबोझ अनुसार पर्याप्त दरवन्दि व्यवस्था गरि सहि काममा योग्य र अनुभवी कर्मचारी व्यवस्था गरिनु पर्ने र दरबन्दि पूर्ति वा कर्मचारी अपर्याप्त भई बाह्य श्रोतबाट पूर्ती गर्नु परेमा मूख्य काम र सहायक काम छुट्याई मूख्य काममा आन्तरिक श्रोत र सहायक काममा बाह्य श्रोतका कर्मचारीलाई काममा खटाईनु पर्दछ । कर्मचारी दरबन्दि तालिका अनुसार निर्देशक १, कम्प्यूटर ईन्जिनियर ३, कम्प्यूटर अफिसर १ र व्यक्तिगत कन्सल्टेन्ट ३ रहेकोमा एक कम्प्यूटर ईन्जिनियर रिक्त रहेकोमा ईजीपि सन्चालन तथा मर्मत सहायतामा डिजीएम मार्केट यूएसए र डिजीएम मार्केट नेपालको जेभी संग २०७५ बैशाखमा २ वर्षिय सम्झौता भई ३ राष्ट्रिय र २ अन्तर राष्ट्रिय परामर्शदाता तथा सहायता कक्ष सेवामा आईटी डिफेन्स प्रा.लि. नामक संस्थासंग सम्झौता गरि काममा लगाएको देखियो । सूचना प्रविधि शाखामा इजिपि हेल्पडेस्क र सूचना प्रविधिका डाटावेश, प्रणाली प्रयोग, मर्मत सम्भार तथा विकासका कार्यहरुसमेत मुख्य कार्य तथा सहायक कार्य(कोर एरिया एण्ड नन कोर एरिया छुट्याई) नछुट्याई बाह्य श्रोतका कर्मचारीहरुबाट काम गराएको छ । यसबाट सूचना तथा तथ्यांकहरु अन्यत्र चुहावट हुनसक्ने, बाह्य श्रोतमा परनिर्भरता बढ्ने जोखिम रहन्छ ।

३.७ **कर्मचारी तालिम :** सूचना प्रविधिको तालीम सम्बन्धी योजना तयार गरी सूचना प्रविधि(ई-जिपी) प्रणाली संचालन गर्ने कर्मचारी तथा आवद्ध प्रयोगकर्ताहरुलाई सुरक्षा जागरण(सेक्यूरिटी अवारनेस) सम्बन्धि आवश्यक तालिम संचालन गरी प्रयोग गर्न सक्षम तुल्याउनु पर्दछ । पाईलट प्रोजेक्टको रुपमा २०७३ बैशाख २ बाट शुरु गरिएको ई-जीपी प्रणाली २०७४ श्रावण १ देखि पूर्णरुपमा कार्यान्वयनमा रहि २०७४।७५ मा १५५० समेत हालसम्म करिब ६००० जना लाभग्राही तथा प्रयोगकर्तालाई जागरण तालिम प्रदान गरेको बुझियो । तर सूचना प्रविधि निर्देशकसंगको छलफलमा कार्यालयको छुट्टै तालीम नबनाएको र कर्मचारीहरुलाई आवश्यकताको आधारमा तालीम दिने गरेको, आर्थिक वर्ष २०७४।७५ मा कार्यालयले प्रणाली संचालन गर्ने कर्मचारीलाई कुनैपनि किसिमको तालिम नदिएको र तालिमका लागि बजेट व्यवस्था पनि नभएको बुझियो । यसबाट मूख्य कर्मचारीहरु नयाँ थप तथा विस्तारीत प्रविधिबाट बन्चित हुने जोखिम रहन्छ ।

३.८ **हेल्पडेस्क** : कार्यालयले उपयोगकर्ताहरुलाई सूचना प्रविधिमैत्री वातावरणमा परेका समस्याहरु तत्काल र पर्याप्त रुपमा विश्लेषण गरि सूचना प्रविधि सहायक मार्फत सुल्झाउन हेल्पडेस्क सेवाको व्यवस्था गरेको हुनु पर्दछ । कार्यालयले हेल्पडेस्क प्रयोगजनका लागी सिफल काठमाण्डौंका आईटि डिफेन्स प्रा.लि. सँग गरेको सम्झौतामा ई-जिपी सफ्टवेयर प्रणालीका प्रयोगकर्ताहरुलाई प्राविधिक निर्देशन तथा हेल्पडेस्कमा आएको समस्या पहिचान गरी (म्याल फंक्सन, परफोरमेन्स प्रोबलम तथा डाटा करप्सन) जस्ता समस्याहरु समाधानको लागि कार्यालयको आईटी समुहलाई पठाउनु पर्ने व्यवस्था छ । उपयोगकर्ताहरुले टेलिफोनबाट सोधनी गर्ने तथा उपयोगकर्ता आवश्यकता अनुसार सम्पर्कमा आएमा ई-जीपी प्रयोगको प्रशिक्षण गर्ने गरेको देखियो । तर कम्पनीले सफ्टवेयरमा आएका समस्याहरु र समाधानका लागि कार्यालयको आईटी समूहलाई जानकारी दिएको वा आफैले समाधान गरेको अभिलेख तथा समस्या पहिचान र समाधान गर्न टिकट पद्धति(टिकेटिङ्ग सिस्टम) राखेको छैन । त्यस्तै यो वर्ष १३२५ लाभग्राहीलाई सेवा प्रदान गरेको अभिलेख रहेकोमा समस्या पहिचान तथा समाधानको अवस्थाको अभिलेख राखेको छैन । जसले यथार्थ लाभग्राही तथा उपयोगकर्ताहरुले प्रणालीमा परेको समस्या समयमा समाधान(रियल टाईम मनिटोरिङ्ग) हुने कार्यमा असर परेको छ ।

३.९**नियमितता परीक्षण :** कार्यालयमा प्रयोग गरिएको सूचना प्रविधि प्रणालीको सूरक्षा मापदण्ड तथा हार्डवेयर र सफ्टवेयर नियन्त्रणहरु ठीकसँग कार्यान्वयन भएको सुनिश्चत गर्नका लागि सन्चालन प्रणालीहरु अनुभवी सिस्टम ईन्जिनियर, सफ्टवेयर प्याकेजबाट परिक्षण, पेनेट्रेसन टेष्ट, सुरक्षा मापदण्ड र सन्चालन मापदण्ड बाट नियमितताको जाँच गरिनु पर्दछ । कार्यालयले बाहिर सञ्जालहरु फायरवालद्धारा ब्लक गरिएको, अवाँछित पोर्टहरु डिसेबल गरिएको, अवाँछित गतिविधिहरुलाई आईपि एर्डेस मार्फत ब्लक गरिएको लगायतका कार्य गरी व्यवस्थित गर्ने प्रयास गरिएको, अन्य नेटवर्कसंग भर्चुअल प्राईभेट नेटवर्क(भिपीएन) मार्फत मात्रै सम्पर्क गर्ने गरिएको र नेटवर्क तथा एप्लिकेशन प्रणालीको अनुगमन परिक्षणका लागि पेनडोरा तथा जिनोस(ओपन सोर्स) औजार प्रयोग गरेको जनाएको छ । तर कार्यालयले यस सम्बन्धि स्वीकृत नीति बनाएको छैन । यसबाट सुरक्षा मापदण्डका लागि अवलम्बन गर्नुपर्ने कार्यहरु बाद्यकारी नभएको र प्रविधिका कर्मचारीहरुले गर्नसक्ने गलत कार्यकालागी जिम्मेवार बनाउन सकिने अवस्था रहदैन ।

३.१० **उपयोगकर्ता प्रक्रिया(यूजर म्यानूअल/प्रोसिडुअर) :** कार्यालयले ईजीपी प्रणाली सन्चालनकालागी बोलपत्रदाता, बैंकर लगायत लाभग्राहीकालागी उपयोगकर्ता दिग्दर्सन(युजर म्यानुअल) तयार गरेको हुनु पर्दछ । कार्यालयले इजिपी निर्देशिका र बोलपत्रदाता, बैंकर लगायत लाभग्राहीकालागी यूजर लग म्यानुअल तयार गरि लाभग्राहीको जिम्मेवारी निर्धारण गरेको छ । तर युजर म्यानुअल बनाएको छैन । यूजर म्यानुअलको अभावमा अनधिकृत पहुँच हुने, संवेदनशिल तथ्यांक तथा सूचनाहरुको चुहावट(डिसक्लोजार) तथा परिवर्तन (मोडिफिकेसन) हुने जोखिम रहन्छ ।

३.११**पासवर्ड :** सूचना प्रविधि प्रणालीका प्रणाली सन्चालक (सिस्टम एडमिनिस्ट्रेटर), साधारण उपयोगकर्ता तथा कर्मचारीहरुलाई अक्षर अङ्क तथा सङ्केत सहितको मजबूत पासवर्डकालागी सजिलै सम्झन सकिने, जटिल र सुरक्षित युजर नेम वा आईडी तथा निस्चित समय पछि पासवर्ड लाई अनिवार्य रुपमा परिवर्तन गर्नुपर्ने व्यवस्था, राउटर, फायरवाल तथा वायरलेस आदि हार्डवेयर तथा सफ्टवेयरका डिफल्ट पासवर्ड परिवर्तन गर्नू पर्ने व्यवस्था सहितको पासवर्ड नीति बनाएको हुनु पर्दछ । सूचना प्रविधि निर्देशकका अनुसार पासवर्ड नीतिको ड्राफ्ट तयार गरेको, व्यवहारमा ८ डिजिटको पासवर्ड बनाउने गरेको, पटक पटक गलत पासवर्ड प्रयोग गरेमा ब्लक गर्ने व्यवस्था रहेको र निर्देशिकाको दफा १६ अनुसार ओ.ट.पी(वान टाईम पासवर्ड) को कार्यान्वयन गरेको भनाई छ । तर पासवर्ड नीति, डिफल्ट पास वर्ड नीति स्वीकृत भएको छैन । तर फायरवाल, सुरक्षा व्यवस्था (ईनक्रिपसन, कि लगर) को पासवर्ड निश्चित समयमा परिवर्तन गर्नु पर्ने वाद्यकारी व्यवस्था छैन । बोलपत्रदाता तथा लाभग्राहीलाई ओ.टी.पी.लाई ईमेल वा एसएमएस बाट पठाउने गरेकोमा अनिवार्य पासवर्ड परिवर्तन गर्नुपर्ने वा स्वाचालित रुपमा पासवर्ड समाप्त(अटोमेटेड सिस्टम फर पासवर्ड) हुने व्यवस्था रहेको छैन । पासवर्ड नीतिको अभावमा ह्याकरले सूचना तथा तथ्याङ्क चुहावट एवं प्रणालीलाई नोक्सानी पुचाउने जोखिम रहन्छ ।

३.१२ **कार्य विभाजन :** प्रणाली सञ्चालनका लागि प्रयोगकर्ता तथा प्रयोगकर्ताहरुको कामको स्पष्ट कार्य विवरण तयार गरिएको हुनुपर्दछ । कार्य विभाजन तर्फ एप्लिकेशन युजरतर्फ कार्यालय स्वयं (सुपर युजर), अन्य सरकारी निकाय (एडमिन, क्रियटर-यूजर-एप्रुभर-एकाउन्टेन्ट), बाणिज्य बैंकहरु (सेन्टर-मेकर-चेकर) र बोलपत्रदाताहरु - युजर) तथा सिस्टम यूजरतर्फ कार्यालयको आई टि ईन्जिनियर तथा विशेषज्ञको सिस्टम एडमिनिस्ट्रेटर गरि वर्गीकरण गरेको छ । एप्लिकेशन यूजरका लागि कार्यालयले निर्देशिका अनुसार कार्यान्वयन गरिएको जनाएको छ । तर सिस्टम यूजरकालागी काम कर्तब्य सहितको स्पष्ट व्यवस्था गरिएको छैन ।

एप्लिकेशन युजर अन्तरगत कार्यालय र नबिल बैक विच भएको सम्झौताको दफा ६(ख) मा बोलपत्रदाताले बोलपत्र सम्बन्धि विद्युतीय प्रति(ईलोक्ट्रोनिक कपी) बैंकको ड्यासबोर्डमा अपलोड गरे पछि २ कार्य दिनभित्रमा बोलपत्र दस्तुर र बोलपत्र जमानतको प्रमाण भिडान गरी कार्यालयलाई प्रणालीबाट जानकारी दिनुपर्ने शर्त रहेका छ । लेखापरिक्षणको क्रममा उक्त बैकको ३८०९४ वटा बैंक निर्देशन परीक्षण गरिएकोमा २

दिन भित्रमा १७००९ (४४ प्रतिशत) र २ दिनभन्दा बढि समय लगाएर २१८९५(५६ प्रतिशत) भिडान गरेको देखियो । काम कर्तव्यको स्पष्ट कार्य विवरण नबनाएकोले कर्मचारीहरु बीचको उत्तरदायित्व बहन नहुने तथा निश्चित समयमा कार्य सम्पन्न नहुने जोखिम रहेको छ ।

३.१३**लग ईन तथा लग आउट** : सफ्टवेयर सञ्चालन सम्बन्धमा सफ्टवेयर सञ्चालन हुन छोडेको निश्चित समयावधी पश्चात स्वतः एप्लिकेशन बन्द हुने, गलत लग ईन वा लग आउट पासवर्ड प्रयोग गरेमा निश्चित प्रयास पछि स्वत व्यवस्था सहितको लग ईन लग आउट नीति हुनु पर्दछ । लेखापरीक्षणमा प्रयोग नभएमा करिव १ घण्टा अवधिपछि स्वत लगआउट हुने र ५ पटकभन्दा वढि गलत पासवर्ड प्रयोग गरेमा १५ मिनटकालागी लक हुने व्यवस्था रहेको करिब एक घण्टा समयवधि पश्चात मात्र(स्क्रिन सोर्ट आउट) हुने गरेको देखियो । तर लग ईन र लग आउट नीति रहेको छैन । जसले गर्दा सफ्टवेयर सञ्चालनमा जोखिमको बढोत्तरी हुने सम्भावना रहन्छ ।

३.१४ **अडिट लग र अनुगमन :** प्रणाली तथा एप्लिकेशनमा गरेका कामहरुको अभिलेख अडिट लग राखि नियमित रुपमा अनुगमन गर्ने र अनधिकृत क्रियाकलाप नियन्त्रण गर्ने गरिनु पर्दछ । कार्यालयले आईटि टिमले परामर्शदातालाई गिटल्याब नामक सफ्टवेयर प्रयोग गरि आन्तरिक समस्याहरुको प्रकृति, समय र अवस्थाको अडिट लग राखेको देखियो । तर ई-जिपी सफ्टवेयरको प्रयोगकर्ताको अडिट लग राख्ने गरेको छैन । प्रणाली प्रयोगमा कुनै समस्या देखिए लाभग्राहीले टेलिफोन मार्फत बाह्य श्रोतबाट नियुक्त हेल्पडेक्स सन्चालकलाई आग्रह गर्ने र टेलिफोनबाट नै समाधान गर्ने गरेको बुझियो । तर नियमितरुपमा प्रयोगकर्ताको पुनरावलोकन,, सफ्टवेयर सन्चालन गर्ने कर्मचारीको अभिलेख, इजिपिका लाभग्राही तथा आईटि कर्मचारीहको अडिट लग पुनरावलोकन गर्ने गरेको देखिएन । हेल्पडेक्सबाट पेश भएको अभिलेख अडिट लगको रुपमा रहेको छैन ।

३.१५ **नवप्रवेशी तथा छाडनेहरुको व्यवस्थापन** : कार्यालयमा प्रयोग गरिएको सफ्टवेयर सञ्चालनको लागि नयाँ प्रवेशीलाई नयाँ यूजर आईडी तथा पासवर्ड दिने तथा अन्यत्र जाने कर्मचारीको तत्काल युजर आईडी तथा पासवर्ड स्थगन(डिसेबल) गरी सुरक्षित व्यवस्थापन गरिनु पर्दछ । कार्यालयले नवप्रवेशी कर्मचारीलाई अभिमुखिकरणसहित युजरनेम र पासवर्ड दिने गरेको, छाडेर जानेको युजरनेम र पासवर्ड ब्लक गर्ने गरेको तथा प्रणाली प्रयोगकर्ता (सिस्टम युजर) भए उसलाई दिएको युजर आईडि र पासवर्ड रमाना हुने एक दिन अगावै बन्द गर्ने भनिएता पनि सोको अभिलेख राखेको छैन । यस सम्बन्धि नीति नरहेकोले कार्यरत कर्मचारी अन्यत्र सरुवा भएमा जोखिम रहन सक्छ ।

३.१६ **प्रणाली सञ्चालक (सिस्टम एडमिनिस्ट्रेसन)** : प्रणाली सन्चालन सम्बन्धि अधिकार तथा अन्य सुविधाहरु कार्य विवरण अनुसार कार्यालयका आन्तरीक श्रोतका सीमित व्यक्तिहरुलाई दिईएको हुनुपर्दछ र प्रणाली सञ्चालकमा सुपर युजर राईट रहेको हुन्छ । कार्यालयले प्रणाली सन्चालक सम्बन्धि अधिकारहरु बाह्यश्रोतका परामर्शदाता कम्पनी डिजि मार्केट कम्पनिका दुई विशेषज्ञलाई दिएको देखियो । बाह्यश्रोतबाट मुख्य क्रियाकलापमा विशेषज्ञ संलग्न गराउँदा प्रयागेकर्ताको सम्वेदनशील तथ्यांक तथा सूचनाहरु चोरिने, हराउने तथा जालसाझ हुने जोखिम रहन्छ ।

३.१७ **एप्लिकेशन नियन्त्रण** : सूचना प्रविधि प्रणाली सन्चालनमा सूचना, कारोबार तथा तथ्याङ्कहरुलाई पूर्ण, शुद्ध, सुरक्षित र आधिकारिक रुपमा राख्न तथा स्थान्तरण(क्याप्चर एण्ड ट्रान्सफर) गर्न नियन्त्रणको वातावरण - कन्ट्रोल ईनभ्यारेमेण्ट) हुनु पर्दछ । नियन्त्रण वातावरणको लागि प्रणाली नक्शा(सिस्टम म्याप) सहितको आधिकारिक प्रयोगकर्ताको सूची(अथोराईज्ड युजर लिस्ट), स्ट्याण्डर्ड इन्पुट फर्म, फरमेट परीक्षण(फरमेट चेक्स), रेन्ज परीक्षण(रेन्ज चेक्स), रिजनेबलनेस चेक, परनिर्भरता परीक्षण, डिजिटको उपयोग, परीक्षण तथा सामान्य व्यवस्थापन पुनरावलोकन(जर्नल म्यानेजमेन्ट रिभ्यू), प्रक्रियाको स्वीकृत अभिलेख समेत रहनु पर्दछ । सूचना प्रविधि लेखापरीक्षणमा एक्टिभिटी डायग्राम लेखापरीक्षणमा पेश भएन । कार्यालयले नियन्त्रण

बातावरणको लागि प्रणाली नक्शांकन(सिस्टम म्याप) बनाएको छैन । सूचना प्रविधि निर्देशकका अनुसार प्रणालीलाई लाईभ सर्भरमा लैजानुपूर्व लाभग्राहीहरुलाई परिक्षणको रुपमा प्रयोग(युजर एसप्टेन्स टेस्ट युएटी)गराएको जनाएतापनि सो सम्बन्धि प्रतिवेदन तयार नगरेको र उक्त प्रतिवेदनमा उल्लेख भएका सुझावहरुको कार्यान्वयन अवस्था समेत तयार गरेको छैन । यसबाट तथ्याङ्क(डाटा) तथा कारोबारको निष्ठामा असर पर्नसक्छ ।

३.१८ **एन्टिभाइरस** : सूचना प्रविधि प्रणालीलाई हानी पुऱ्याउन सक्ने संकास्पद क्रियाकलाप तथा भाईरस/म्यालिसियस प्रोगाम ईत्यादिलाई नियन्त्रण गर्ने, पत्ता लगाउने र हटाउने एन्टि भाइरस, प्रयोग गर्ने नीति तयार गरि कार्यान्वयन गरिनु पर्दछ । कार्यालयले ई-जिपी सफ्टवेयरको एप्लिकेशन कन्ट्रोल प्रणालीमा एन्टिभाइरस राखेको छैन । डेभलेपरको डिभाईसमा बजारमा उपलब्ध भएको एन्टिभाइरस राख्ने गरेको तर एप्लिकेसन कन्ट्रोल सर्भरका लागि कन्सलटेन्ट/डेभलेपर्सले एन्टिभाइरस राख्न नपर्ने जनाएकोले नराखिएको भनाई रहेता पनि सो सम्बन्धि निर्णय भएको देखिएन । ई-जिपीमा एन्टिभाईरस प्रयोग नगरिनुले बोलपत्रदातालगायत लाभग्राहीहरुले अपलोड गरेका फायलहरु स्यान नहुने भाईरस आक्रमणबाट प्रणालीका तथ्यांक तथा सुचनाहरु काम नलाग्ने (करप्टेड/ईर्नाफिक्टेड) हुने जोखिम रहन्छ ।

३.१९ **डाटावेश सुरक्षा** : सूचना प्रविधिको सूचना, तथ्यांक तथा सफ्टवेयर सुरक्षाको लागि विशेष सुरक्षाको व्यवस्थाहरु अपनाउनु पर्दछ । ई-जिपी सफ्टवेयर सम्बन्धमा कार्यालयले त्यस्तो व्यवस्था गरेको देखिएन । जसले गर्दा सफ्टवेयर तथा डाटाको सुरक्षामा जोखिम सृजना हुन सक्दछ ।

३.२० **पूर्वाधार पहुँच सुरक्षा विधि(फिजिकल एक्सेस सेक्यूरिटि प्रोसिडिअर)** : सूचना प्रविधि सम्बन्धि हार्डवेयर तथा सफ्टवेयरमा समानरुपमा प्रयोग हुने गरि भौतिक सुरक्षा विधि स्वीकृत गरी अवलम्बन गरिएको हुनुपर्दछ । कार्यालयको पूर्वाधार पहुँच सुरक्षाकालागी स्वीकृत नीति तथा विधि रहेको छैन । डाटावेशको सुरक्षाको लागि डाटा सेन्टर, डिजास्ट्रर रिकभरी सेन्टर तथा डाटा ब्याकअपको उचित व्यवस्थापन गरिएको हुनुपर्दछ । ई-जिपी सफ्टवेयरको डाटा सेन्टर राष्ट्रिय सूचना प्रविधि केन्द (आइटिसी) को सरकारी एकीकृत तथ्याङ्क केन्द्र(जिआइडिसी) मा भएता पनि डाटा व्याकअपको लागि कार्यालयले पेन ड्राईभ जस्ता डिभाईस मार्फत डाटा ट्रान्सफर गर्ने गरेको छ । कार्यालयले सफ्टवेयरको नियमित पुनरावलोकन गर्ने गरेको छैन । जिआईडिसीमा रहेको सार्वजनिक खरिद अनुगमन कार्यालयको भौतिक पूर्वाधारको सुरक्षाकोलागी एनआईटिसीमा निर्भर रहेको छ । स्वीकृत पूर्वाधार पहुँच सुरक्षा विधिको अभावमा प्रविधिको पूर्वाधारमा अन्य व्यक्तिको अनधिकृत पहुँचको जोखिम रहेको छ । अत कार्यालयको सूचना प्रविधिको भौतिक पूर्वाधार सुरक्षाका लागि नीति तथा विधि स्वीकृत गराई कार्यान्वयन गरिनु पर्दछ ।

३.२१ **पूर्वाधार सुरक्षा** : कार्यालयको सूचना प्रविधि सम्बन्धि पूर्वाधारहरु जस्तै हार्डवेयर तथा सफ्टवेयर जडान गरिएको कक्षमा प्रवेशका लागि निश्चित व्यक्तिहरु बाहेक अन्यलाई प्रवेश निषेध गरिएको तथा उक्त कक्षमा प्रवेशका लागि विशेष सुरक्षा पास(सेक्युरिटि पास) तथा आगन्तुक पुस्तिका(भिजिटर लग्स) व्यवस्था गरिएको हुनु पर्दछ । लेखापरिक्षणको क्रममा सर्भर कक्ष तथा मा प्रवेश गर्ने र बाहिरिनेहरुका लागि म्यानुअल लग राखेको देखियो । कार्यालयको सर्भर रहेको कक्ष खुल्ला राखेको छ । हातले राखेको म्यानुअल लग्स स्वतन्त्र तथा भरपर्दो रहँदैन र यसले महत्वपूर्ण एवं सम्वेदनशील हार्डवेयर उपकरणमा अनधिकृत पहुँच भई चोरी नोक्सानीको जोखिम रहन्छ ।

३.२२ **अनुगमन** : कार्यालयले स्वचालित कार्य सन्चालन मा अनधिकृत फाइल, तथ्यांक वा गल्तिहरुलाई विश्लेषण गरि सफ्टवेयर तथा तथ्यांकहरुबाट हटाउन तथा रोक्नकालागी नियमित अनुगमन गरिनु पर्दछ । कार्यालयले ईजिपी सफ्वेयरका विशेष जोखिमहरु मूल्यांकन गर्ने गरेको छैन । लाभग्राहीहरुको समस्याहरु कार्यालयका आफ्नै कर्मचारीहरुबाट समाधान गर्ने र नसकेमा बाह्य श्रोतको निकायमा पठाउने र विश्लेषण परिक्षण गरि

समाधान गरेको बुझियो । तर ई-जिपी सफ्टवेयरको समग्र मूल्यांकन गरिएको छैन । यसबाट ई-जिपी प्रणालीको कार्यसम्पादनमा प्रभाव पार्नसक्ने समस्या तथा घटनाहरु(मेजर ईस्यु/ईन्सिडेन्ट) को जोखिम रहन्छ । यसले सामान्य व्यवसायिक कार्यसन्चालनमा दिला हुने तथा प्रणाली समयानुकुल अद्यावधिक नहुने हुन्छ ।

३.२३ **व्याकअप नीति :** कार्यालयले सबै अभिलेख, सूचना तथा तथ्याङ्कहरु निरन्तर एवं दैनिक रुपमा सुरक्षित हुने गरी तीन तह(थ्री जेनरेसन/साईकल) को व्याकअप सूचनाको व्यवस्था गरि सबै तथ्याङ्क तथा अभिलेखहरु निरन्तर परिक्षण गरिएको हुनु पर्दछ । कार्यालयले दैनिक दुई पटक २० मिनट समय लगाई व्याकअप गर्ने गरेको र राष्ट्रिय सुचना प्रविधि केन्द्रको सरकारी सुचना तथ्याङ्क केन्द्रमा व्याकअप गर्ने गरेको देखियो । तर कार्यालयले व्याकअप सर्भर तथा तथ्याङ्क परीक्षण नगरी राख्ने गरेको छ । उचित एवं नियमित परिक्षण नगरी भण्डारण गरेको अभिलेख तथा तथ्याङ्क पुन प्रयोग गर्न नमिल्ने जोखिम रहन्छ ।

३.२४ **तेश्रोपक्ष** : कार्यालयको कायबोझ तथा आवश्यकता अनुसार स्वीकृत व्यवस्थापकीय निर्णयको आधारमा तेश्रो पक्ष नियुक्त गरिनु पर्दछ । कार्यालयले सहायता कक्ष व्यवस्थापक(हेल्प डेस्क म्यानेजर), प्रणाली व्यवस्थापक (सिस्टम एडमिनिष्ट्रर), नेटवर्क व्यवस्थापक, डाटाबेस व्यवस्थापक(डाटावेश एडमिनिष्ट्रर) एसएमएस सेवा प्रदायक आदि कार्यका लागि बाह्य श्रोतबाट तेश्रोपक्ष नियुक्त गरेको छ । ई-जिपी प्रणाली सन्चालनमा बाह्यश्रोतका कम्पनीमा अधिक निर्भर रहेको देखियो । तेश्रोपक्षले सेवा प्रवाहको सम्झौताको नवीकरण नगरेको अवस्थामा कार्यालयको कार्यसञ्चालनमा हानि पुग्ने तथा कार्यालयका आन्तरिक श्रोतका कर्मचारीहरुमा आत्म विश्वासको जोखिम रहन्छ । अतः तेश्रोपक्ष मार्फत प्राप्त सेवाको कार्यसम्पादनको मूल्याङ्कन समयानुकुल नवीकरण गर्ने तथा आन्तरीक कर्मचारीहरुको क्षमता विकास गरि तेश्रोपक्ष माथिको परनिर्भरता नियन्त्रण गरिनु पर्दछ ।

३.२५ **ईन्टरफेस** : कार्यालयले नेटवर्क, डिस्कस वा टेप्स मार्फत पूर्ण तथा शुद्ध तथ्याङ्कहरु स्थान्तरण गरेको र नेटवर्क मार्फत स्थान्तरण हुनेमा स्वचालितरुपमा गल्ति पत्तालगाउने र सुधार गर्ने सुविधा रहेको हुनु पर्दछ । परिक्षणको क्रममा तथ्याङ्कहरु सोझै डाटाबेसमा जाने र अपलोड तथा स्थान्तरणमा हार्ड डिस्क प्रयोग हुने गरेको छ । तर अपलोड पूर्व भाईरस परिक्षणका लागि डाटा स्क्यान गर्ने प्रणाली रहेको छैन । स्थान्तरण गरिएको तथ्याङ्कको शुद्धता र पूर्णताको परिक्षण गर्ने निर्देशिका तथा नीति तयार गरेको छैन । पुनरावलोकन गर्ने पद्धती नरहेकोले शुद्ध तथा पुर्ण तथ्याङ्क स्थान्तरणमा विश्वस्त नहुने जोखिम रहेको छ ।

३.२६ **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 । कार्यालयले सम्पूर्ण हार्डवेयर तथा सफ्टवेयरहरुको आगलागी, बाढि, भुकम्प तथा अनियमित विद्युत आपूर्तीकालागि राष्ट्रिय सुचना प्रविधि केन्द्रमा रहेको सरकारी सुचना डाटा केन्द्रमा निर्भर रहेको पाईयो । तर सरकारी एकिकृत डाटा सेन्टरमा रहको पूर्वाधार वाढी, भुकम्प तथा अनियमित विद्युत आपूर्ती व्यवस्था सन्तोषजनक हुन सक्ने पूर्वाधार व्यवस्थाको अभिलेख कार्यालयमा रहेको देखिएन । यसबाट कार्यालयको सूचना तथा तथ्याङ्क नोक्सानी हुनसक्ने जोखिम रहेको छ ।

३.२७ **सेक्युरिटी लग्स** : कार्यालयले सूचना प्रविधिको प्रयोगमा आईपरेका सबै किसिमका सुरक्षा चुनौती(सेक्यूरिटि थ्रेट) को अभिलेख राख्ने र उच्च व्यवस्थापनबाट विश्लेषण गरि समाधान गर्ने व्यवस्था हुनु पर्दछ । कार्यालयले सेक्यूरीटि लग्स राख्ने गरेको छ । तर उक्त लग्स अनुगमन गर्ने गरिएको छैन । यसबाट नेटवर्कमा अनधिकृत गतिविधि, अनधिकृत परिमार्जन पत्ता नलाग्ने जोखिम रहन्छ ।

३.२८ **सम्पत्ति अभिलेख** : सुचना प्रविधिमा प्रयोग भाएका सबै हार्डवेयर तथा सफ्टवेयरको सम्पत्ति अभिलेख राख्ने र नियमित भौतिक परिक्षण गरि अभिलेख अद्यावधिक राखेको हुनु पर्दछ । कार्यालयले हार्डवेयर तथा सफ्टवेयरको अभिलेख अन्य सम्पत्तिसंग राखेको र सो पनि स्पष्ट रहेको छैन । सरकारी सूचना तथ्याङ्क केन्द्र मा

रहेको पूर्वाधारको मासिक रुपमा अवलोकन गर्ने गरको छ । कार्यालयले सुचना प्रविधिसंग सम्बन्धित हार्डवेयर तथा सफ्टवेयरहरुको वर्गीकरण 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 ।

३.२९ **तथ्याङ्क धुल्याउने :** कार्यालयले कागज,चुम्बकीय, श्रव्यदृश्य, युएसवी स्टोरेज, पुराना कम्प्युटर र ल्यापटप आदीमा रहेका सम्वेदनशील सुचना तथा तथ्याङ्कहरु स्वीकृत कार्यविधि अनुसार धुल्याएको हुनु पर्दछ । कार्यालयले हालसम्म तथ्याङ्क धुल्याउने कार्यहरु गरेको छैन र कार्यविधि तयार गरेको पनि छैन । तथ्याङ्कहरु नधुल्याईएमा तथ्याङ्क रहने स्थान(डाटा स्टोरेज स्पेस) को अभावको जोखिम रहन्छ । अत अनावश्यक तथ्याङ्कहरु पहिचान गरि उच्च व्यवस्थापनको स्वीकृतीमा धुल्याईनु पर्दछ । परीक्षणको क्रममा डिभाईसको ७८ प्रतिशत स्पेश प्रयोग भईसकेको देखिएको छ ।

३.३० **व्यवसाय निरन्तरता योजना र प्रकोप पुनःस्थापना योजना(बीसीपी तथा डीआरपी) :** कार्यालयले सूचना प्रविधिको व्यवसाय निरन्तरता योजना(बिजनेश कन्टिन्युनिटि प्लान) र प्रकोप पुनःस्थापना योजना(डिजास्टर रिकभरी प्लान) तयार गरी त्यसको प्रभाव विश्लेषण गर्नु पर्दछ । कार्यालयले व्यवसाय निरन्तरता योजना तथा प्रकोप पुनःस्थापना योजना तयार गरेको छैन । कार्यालयको प्रकोप पुनःस्थापनाका लागि साईट उपलब्ध नभएको र जिआईडिसिका लागि हेटौडामा स्थान उपलब्ध भएको जनाएको छ । यी योजनाको अभावमा बाह्य चुनौती, साईवर आक्रमण, प्राकृतिक प्रकोप आदी अवस्थामा ईजिपी प्रणालीको निरन्तरतामा अवरोधको जोखिम रहन्छ । यसबाट सुचना तथा तथ्याङ्कको विश्वसनियता तथा निष्ठतामा असर पर्दछ ।

प्रणाली कार्यान्वयन तथा सन्चालन : यसमा निम्न व्यहोराहरु देखिएका छन् :

३.३१ **केन्द्रीय अभिलेख :** कार्यालयमा प्रयोगमा रहेका सफ्टवेयरहरु नेपाल सरकारको सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सन्चालन) निर्देशिका, २०७१ को दफा ४ अनुसार सुचना प्रविधि विभागमा अभिलेखिकरण गर्नुपर्ने व्यवस्था छ । लेखापरीक्षणको क्रममा कार्यालयमा प्रयोग भएका सफ्टवेयरहरुको सूची माग गरिएकोमा पेश गरेन । कार्यालयले सूचना प्रविधि विभागमा ई-जिपी सफ्टवेयरलाई अभिलेखिकरण गरेको देखियो तर कार्यालयले उपयोग गरेका अन्य सफ्टवेयरहरु एफएमआईएस, आरएमआईएस, ई-एटेनडेन्स ,पीपीएमआईएस आदि सूचना प्रविधि विभागमा अभिलेखिकरण गरेको देखिएन । यसबाट सफ्टवेयरको बैधानिकता, नियमितता तथा अभिलेखिकरणमा असर परेको छ । अतः कार्यालयमा प्रयोग भएका वेभसाईट लगायत सबै प्रकारका सफ्टवेयरहरु सूचना प्रविधि विभागमा अभिलेखिकरण गरिनु पर्दछ ।

३.३२ **अनुकुलित/परिमार्जित सूचना प्रविधि प्रणाली(कस्टुमाईज्ड/बीस्कोप आईटी सिस्टम) :** कार्यालयले सूचना प्रविधि प्रणालीलाई कार्यालयको कामको रणनीति, परिभाषित आवश्यकता तथा मापदण्ड, जोखिम विश्लेषण, लागत - लाभ विश्लेषण, सुरक्षा जोखिम मूल्याङ्कन अनुसार प्रणाली विकास, परिमार्जन तथा सुधार गर्ने गरि प्राथमिकता निर्धारण गरिनु पर्दछ । सुचना प्रविधि निर्देशकका अनुसार विद्युतीय सरकारी खरिद प्रणालीलाई सार्वजनिक खरिद ऐन अनुसार परिमार्जन गरिएको र सरकारी निकाय, बैंक, बोलपत्रदाता तथा अन्य उपयोगकर्ताको समस्याहरु र सुझावहरु सूचना प्रविधि(आईटि) टिमको पुनरावलोकन तथा छलफल पश्चात स्वीकृत गराई अद्यावधिक, परिमार्जन तथा पुनरावलोकन गर्ने गरेको छ । तर कार्यालयले प्रणाली पुरावलोकन गर्ने निश्चित समय निर्धारण गरेको छैन । अतः कार्यालयले प्रयोगमा आएको सफ्टवेयर सम्बन्धमा नियमित तथा समयानुकुल प्रयोग पश्चात पुनरावलोकन(पोष्ट ईम्प्लिमेन्टेसन रिभ्यु)को व्यवस्था गर्नुपर्दछ ।

३.३३ **उच्च व्यवस्थापन स्वीकृती(सिनियर म्यानेजमेन्ट एप्रुभल) :** सञ्चालित सूचना प्रविधि प्रणालीमा थप विकास तथा परिमार्जन गर्नु परेमा कार्यालयको उच्च व्यवस्थापन तथा सूचना प्रविधि शाखाको स्वीकृत भएको हुनु पर्दछ । कार्यालयको सूचना प्रविधि प्रणालीमा कुनै परिमार्जन गर्नु परेमा टेस्ट सर्भरमा परिक्षण पश्चात प्रणाली

प्रशासकले आईटी शाखाका कम्प्युटर ईन्जिनियरलाई र नीजको सिफारिस पश्चात आईटी निर्देशकले अन्तिम स्वीकृत गर्ने गरेको देखियो । तर प्रणालीमा आवधिक पुनरावलोकन गर्ने व्यवस्था र प्रणाली परिवर्तन गर्दा उच्च व्यवस्थापनको स्वीकृति गराउने गरेको छैन । त्यस्तै सफ्टवेयर प्रणालीमा के के, कहिले र कसले परिमार्जन गरेको भन्ने परिवर्तनको स्वचालित लेखांकन प्रणाली(अटोमेटेड चेञ्ज ट्र्याकिङ्ग सिस्टम) छैन । समयानुकुल पुनरावलोकन नहुनाले निर्धारित समयमा गरिनु पर्ने सुधार नहुन सक्दछ । अतः स्वचालीत अभिलेखाङ्कन प्रणाली जडान गर्ने, निर्धारित समयमा पुनरावलोकन गर्ने तथा परिमार्जन पुर्व उच्च व्यवस्थापनको स्वीकृति गराउने व्यवस्था मिलाउनु पर्दछ ।

३.३४ **कार्य विभाजन :** कार्यालयले सफ्टवेयर प्रणालीको तथ्याङ्कहरुको विकास, परिमार्जन, परिक्षण, कार्यान्वयन र स्थान्तरण(डेभलपमेण्ट, मोडिफिकेशन, टेस्टिङ्ग, डिप्लोएमेण्ट/म्याईग्रेसन) गर्ने कार्य फरक फरक बातावरणमा व्यवस्थित गरेको हुनुपर्दछ । तर ई-जीपी सफ्टवेयर प्रणालीमा तथ्याङ्कहरुको विकास र परिक्षण(डेभलेपर/टेस्टर) एउटै व्यक्ति रहेको छ । जसले गर्दा सफ्टवेयरमा विकास तथा परिमार्जनबाट प्रयोगमा भएको समस्याको पहिचान नभई सफ्टवेयर सञ्चालनमा समस्या आउन सक्दछ ।

३.३५ **उपयगोकर्ता स्वीकृति परिक्षण(यूजर एसप्टेन्स टेस्ट) :** कार्यालयले विकास तथा परिमार्जन गरेको सफ्टवेयर प्रणालीलाई प्रयोगमा लैजानु भन्दा पहिला लाभग्राहीहरुलाई उपयोगमा सहज हुने वा समस्या नआउने सम्बन्धमा उपयोगकर्ता स्वीकृति परिक्षण गराउनु पर्दछ । कार्यालयले ई-जिपी प्रणालीको प्रथम चरण र दोश्रो चरणको सफ्टवेयरको उपयोगकर्ता स्वीकृति परिक्षण(यूजर एसप्टेन्स टेस्ट) गराएको देखिएन । हाल कार्यालयले बाह्यश्रोतको तेश्रोपक्ष डिजी मार्केट प्रा.लि. मार्फत सफ्टवेयर विकास तथा परिमार्जन गरेकोमा सोको उपयोगकर्ता स्वीकृति परिक्षण गराउने चरणमा रहेको जनाएको छ । उक्त परीक्षण नगराई प्रयोग गरिएको ईजिपी प्रणालीको पहिलो र दोश्रो चरणको सफ्टवेयरले कार्यान्वयनको उद्देश्यहासिल नगर्ने जोखिम रहन्छ । अतः प्रणालीमा गरिएका सम्पूर्ण परिमार्जनको स्वचालित अभिलेख राख्ने तथा उपयोगकर्ता स्वीकृति परिक्षण पश्चातमात्र उपयोगमा ल्याउनु पर्दछ ।

३.३६ **परिवर्तन व्यवस्थापन(चेञ्च म्यानेजमेण्ट) :** कार्यालयमा प्रणाली प्राप्ति तथा व्यवस्थापन परिवर्तन तथा प्रणालीमा आकस्मिक परिमार्जन गर्दा नीति अनुसारको पक्रिया अवलम्बन गरिनु पर्दछ । कार्यालयले प्रणाली कार्यान्वयनमा कुनै किसिमको परिवर्तन गर्नु परेमा आईटी डाईरेक्टरको स्वीकृतिमा गर्ने गरेको र प्रणाली प्राप्ति(सिस्टम एक्यूजिसन) गर्नु परेमा सार्वजनिक खरिद अनुगमन कार्यालयका सचिवको सहमति र स्वीकृर्तीमा आईटी टीमसंगको छलफल पश्चात प्राप्ति गर्ने गरेको छ । तर कार्यालयले परिवर्तन व्यवस्थापन(चेञ्च म्यानेजमेण्ट), प्रणाली प्राप्ति(सिस्टम एक्यूजिसन) तथा आकस्मिक प्रणाली परिमार्जन(ईमरजेन्सी सिस्टम मोडिफिकेसन) का विधि तयार गरेको छैन ।

३.३७ **वारेण्टी :** कार्यालयले प्राप्ति गरेका हार्डवेयर तथा सफ्टवेयरको वारेण्टीको सम्झौता समेत गरेको हुनु पर्दछ । कार्यालयले हार्डवेयर तथा सफ्टवेयर खरिद गर्दा सोको स्पेसिफिकेशनमा वारेन्टि हुने जनाएतापनि कार्यालयले वारेन्टि सम्बन्धि अभिलेखहरु राखेको छैन । यसबाट हार्डवेयर तथा सफ्टवेयरको उपयोग अवधिको सुनिश्चितता तथा सञ्चालन/मर्मत लागत बृद्धिको जोखिम बढेको छ ।

३.३८ **प्रयोग पश्चात पुनरावलोकन(पोष्ट ईमप्लिमेन्टेसन रिभ्यू) :** कार्यालयमा प्रयोगमा आएको सफ्टेयर प्रणालीको विकास तथा परिमार्जनको कार्यसम्पादनको निश्चित समयमा प्रयोग पश्चात पुनरावलोकन गरिएको हुनु पर्दछ । जसले गर्दा सफ्टवेयरमा सृजना भएका समस्याको जानकार कार्यालयलाई समयमै हुन्छ । तर कार्यालयले ईजीपL सफ्टवेयर प्रणालीको समय समयमा सफ्टवेयरको पुनरावलोकन गर्ने व्यवस्था गरेको छैन । यसबाट प्रणाली सन्चालनमा आईपरेका(ईर्नासिडेण्ट, बग्स) तथा अन्य विभिन्न समस्याहरु समाधान हुन नसकी

प्रणालीको निरन्तर सन्चालन तथा सुनिश्चिततामा जोखिम रहन्छ । अतः कार्यालयले प्रयोगमा आएको सफ्टवेयर प्रणालीको प्रयोग पश्चात पुनरावलोकन गरि देाीएका समस्याहरु समाधान गर्ने व्यवस्था गर्नुपर्दछ ।

३.३९ **प्रणाली प्रयोगको लागि दर्ता :** विद्युतीय खरिद प्रणाली सञ्चालन निर्देशिका, २०७४ को परिच्छेद-३ को दफा ६ र ७ मा सार्वजनिक खरिद कारोबार गर्ने मन्त्रालय/विभाग वा यस्तै केन्द्रीयस्तरमा रहेका सार्वजनिक निकायहरु प्रणाली सन्चालक(एडमिन युजर) को रुपमा सार्वजनिक खरिद अनुगमन कार्यालयमा, प्रदेश र जिल्ला तथा स्थानीय स्तरका सार्वजनिक निकायहरुले प्रणाली प्रयोगकर्ता(सिस्टम युजर)को रुपमा आफ्नो तालुक कार्यालयको प्रणाली सञ्चालकसँग सम्पर्क गरी प्राप्त निर्देशन बमोजिम दर्ता गर्नुपर्ने र मातहत कार्यालयहरुको सम्बन्धमा तालुक निकायले ई-जिपी फ्टवेयर सञ्चालनको एडमिन युजर आईडी र पासवर्ड तयार गरी मातहत कार्यालयलाई दिनुपर्ने व्यवस्था छ । कार्यालयमा २०७५ आश्विनसम्ममा नेपाल राष्ट्र बैंक, धनगढी, सशस्त्र प्रहरी वल, मोरङ्गआदि समेत १६३४ सार्वजनिक निकायहरु दर्ता भएका छन् । कार्यालयले मन्त्रालयस्तर, विभागस्तर लगायत केन्द्रियस्तरका निकायहरुमात्र दर्ता गर्नुपर्नेमा प्रादेशिकस्तर, जिल्लास्तर र स्थानीयस्तरका निकायहरुसमेतलाई सोझै दर्ता गर्ने गरेको देखियो । प्रादेशिकस्तर, जिल्लास्तर र स्थानीयस्तरका निकायहरुको पासवर्ड तथा युजर नेमहरु तालुक मन्त्रलाय, विभाग तथा केन्द्रियस्तरका निकायहरुले निर्माण गर्नुपर्नेमा सो नगरि सोझै सार्वजनिक खरिद अनुगमन कार्यालयले निर्माण गरि वितरण गरेको छ । यसबाट प्रादेशिक, जिल्ला तथा स्थानीयस्तरका निकायहरु सम्बन्धित मन्त्रालय, विभाग तथा केन्द्रीयस्तर निकायहरु वाईपास भई अनियन्त्रित हुने जोखिम रहन्छ ।

३.४० **सूचना प्रकाशन तथा प्रस्ताव :** ई-जिपी खरिद निर्देशिकाको दफा १३ अनुसार बोलपत्र सूचना प्रकाशन तथा दफा १६ अनुसार बोलपत्रदाताहरुले आफ्नो बोलपत्र प्रस्ताव अनलाईन मार्फत दर्ता गरेको हुनु पर्दछ । कार्यालयहरुले प्रकाशन गरेको बोलपत्र सूचना अनुसार अधिकांश बोलपत्रदाताहरुले बोलपत्र प्रस्ताव पेश गर्दा अपलोड मोडल र अनलाईन दुवै माध्यम मार्फत प्रस्ताव पेश गर्ने गरेको र अधिकांशले एक्सएल फरम्याटमा अनलाईनमा अपलोड गर्ने गरेका छन् । बोलपत्रदाताहरुले बिल अफ क्वाण्टिटिजको बोलपत्र विवरण नभरी आफ्नै ढाँचामा एक्सएलसीट तयार गरी पेश गरेको बोलपत्र प्रस्तावलाई ईजिपि प्रणालीले स्वीकार गरेकोले खरिद प्रणालीको निर्धारित प्रक्रिया अवलम्बन नगर्ने तथा एक्सएल फरमेटमा एकरुपता नहुने जोखिम बढेको छ । अत सवै बोलपत्रको सूचना र बोलपत्र प्रस्ताव अनलाईन प्रकाशन गराउने गरि कार्यालयले एक्सएलसिटको ढाँचा समेत सफ्टवेयर प्रणालीले निर्धारण गर्ने गरि एकरुपता कायम गरिनु पर्दछ ।

बोलपत्रदाताको प्रकार	बोलपत्र संख्या	बोलपत्र रद्द संख्या	एक्सेलमा अपलोड संख्या	दुईवटा खाम प्रद्धति संख्या	एकल खाम पद्धति संख्या
परामर्श सेवा	१५२	०	०	०	१५२
मालसामान खरिद	१९८५	३४	१२८७	०	६६४
निर्माण	५१५९	२७	१२३१	१८१८	२०८३
जम्मा	७२९६	६१	२५१८	१८१८	२८९९

३.४१ **बोलपत्र मूल्याङ्कन,स्वीकृती र भुक्तानी :** ई-जिपी सन्चालन निर्देशिकाको दफा २२ अनुसार बोलपत्र प्रस्तावको मूल्याङ्कन, दफा २३ अनुसार बोलपत्र स्वीकृतिको आशयको सूचना, पुनरावलोकन तथा बोलपत्र स्वीकृतिको पत्र र दफा २८ अनुसार कामको अग्रिम/पेश्की/रनिङ्ग बिल/अन्तिम बिल/क्षतिपूर्ति लगायतका विलहरु अनलाईन मार्फत पेश गर्ने र भुक्तानी दिनुपर्ने व्यवस्था छ । सबै कार्यालयको प्रश्नावली विवरण अनुसार यो वर्ष ७२७६ वटा अनलाईन बोलपत्र सूचना प्रकाशन भएकोमा १३३२ (१८ प्रतिशत) बोलपत्रको मात्र अनलाईन मूल्याङ्कन भएको र मूल्याङ्कित बोलपत्रहरु मध्ये २९० (२१ प्रतिशत) वटा बोलपत्रको स्वीकृती र २०३(१५प्रतिशत) वटा बोलपत्रको आसय पत्र अनलाईन मार्फत गरेको छ । तर कार्यालयहरुले बोलपत्रदाताहरुलाई अग्रिम, पेश्की,

रनिङ्ग विल, अन्तिम विल र प्रोत्साहन भूक्तानीको कार्य विद्युतीय खरिद प्रणाली मार्फत गरेको देखिएन । यसबाट ई-जिपि प्रणालीमा व्यवस्थित बोलपत्र स्वीकती, आशयपत्रको सूचना दिने, पुनरावलोकन गर्ने, अग्रिम तथा पेश्की भुक्तानी, रनिङ्ग तथा अन्तिम विल र क्षतिपूर्ति भुक्तानी गर्ने व्यवस्थाको अनुशरण नहुने जोखिम बढेको छ ।

३.४२**विद्युतीय खरिद प्रणालीको प्रयोग(ईम्प्लीमेन्टेसन अफ ई-जिपी सिस्टम)** : विद्युतीय खरिद प्रणाली सन्चालन निर्देशिका, २०७४ को दफा ३५ मा सार्वजनिक निकायले विद्युतीय प्रणालीबाट खरिद गर्दा अनिवार्य रुपमा सार्वजनिक खरिद अनुगमन कार्यालयले सन्चालनमा ल्याएको विद्युतीय खरिद प्रणालीको मात्र प्रयोग गर्नुपर्ने र रु.२० लाख भन्दा माथिको परामर्श सेवा, रु.६० लाख भन्दा माथिको खरिद र रु.२ करोड भन्दा माथिको सार्वजनिक निर्माणमा अनिवार्य रुपमा विद्युतीय खरिद प्रणालीबाट मात्र खरिद गर्नु पर्ने र सार्वजनिक निकायले खरिद सूचनामा ई-जिपी प्रणालीको एकल पोर्टलमा रहेको बोलपत्र सम्बन्धि कागजातको खरिद सूचनामा र बोलपत्र सम्बन्धी विवरण खण्ड(डाटा सिट) मा सम्पूर्ण खरिद व्यवस्था विद्युतीय खरिद प्रणाली सन्चालन निर्देशिका बमोजिम मात्र हुनेछ भनी उल्लेख गर्नु पर्नेछ भन्ने व्यवस्था गरेको छ । कार्यालयको प्रश्नावली विवरण अनुसार रु.२० लाखभन्दा माथिको परामर्श २३ वटा, रु.६० लाख भन्दा माथिको मालसामान खरिद ३८१ वटा, रु.६० लाखभन्दा माथिको निर्माणकार्य १२४१ वटा र रु.२ करोडभन्दा माथिको निर्माण कार्य ६५६ वटाको अनलाईन बोलपत्र सूचना प्रकाशन भएको देखिएको छ । कार्यालयको अभिलेखमा रहेको विवरण अनुसार निर्देशिकाको अनुशरण नभएको केही उदाहरण निम्न देखिएको छ ।

निकायको नाम	सूचना प्रकाशन मिति	कामको विवरण	बोलपत्र जमानत (२.५ प्रतिशत)	लागत अनुमान	ठेक्का नं
स्थानीय पूर्वाधार विभाग	अक्टोवर २, २०१८	१३,२६,३२,३६ र ४० एमएमको वायर आपूर्ति तथा ढुवानी	अमेरिकी डलर ५५०००	अमेरिकी डलर २२०,००,०००	आईसीबी/टीवी/डब्लुआर /०१-२०१८/१९
कङ्काली नगरपालीका, झापा	श्रावण १४, २०७५	हाइड्रोलिक एक्साभेटर (कम्तिमा १६५ एचपी)	रु २,७५,०००	रु १,१०,००,०००	ककनी/०१/०७५-७६

माथि उल्लिखित उदाहरणमा दुवै बोलपत्रहरुको अनिवार्य रुपमा विद्युतीय माध्यमको प्रयोगबाट मूल्याङ्कन गर्नुपर्ने सीमामा रहेकोमा छ । स्थानीय पूर्वाधार विभागको बोलपत्र सूचनाको सि.नं ६ मा निर्देशिका अनुसार विद्युतीय माध्यमबाट खोलिने भन्ने मात्र र कङ्काली नगरपालीकाको बोलपत्र सूचनाको सि नं ७ मा बोलपत्रदाताको प्रतिनिधिहरुको रोहवरमा बोलपत्र खोलिने उल्लेख गरको छ । यसबाट निर्देशिकाको दफा ३५ को अनुशरण र प्रणाली कार्यान्वयनमा असर पर्ने जोखिम रहन्छ । यसको कारण निर्देशिकाको कार्यान्वयन बाध्यकारी नहुनु हो ।

३.४३**बैंक जमानत** : बैंक ग्यारेन्टीको नियन्त्रण र निरीक्षणका लागि ई-जिपी सफ्टवेयर संयन्त्रमा व्यवस्था गरेको हुनुपर्छ । सरकारी विद्युतीय खरिद प्रणालीको सफ्टवेयर सुचना प्रविधि प्रणालीमा बोलपत्र जमानत तथा कार्यसम्पादन 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 जोखिम बढ्ने देखिन्छ ।

परिच्छेद-४ : सुझाव तथा निष्कर्ष

४.१ लेखापरीक्षणबाट देखिएका उल्लिखित ब्हयोराहरुका सम्बन्धमा निम्न अनुसारका सुझाव कार्यान्वयन गर्नु उपयुक्त देखिन्छ :

4.1.1 **सूचना प्रविधि निर्देशक समिति :** सूचना प्रविधि सम्बन्धमा देखिएका नविन अवधारणा तथा आन्तरिक रुपमा देखिएका समस्या तथा चुनौती उपर निर्णय लिनको लागि कार्यालयमा २०७५।६।९ मा सहसचिवको संयोजकत्वमा ६ सदस्यीय प्राविधिक समिति सूचना प्रविधि निर्देशक समिति गठन गरेता पनि हालसम्म कुनै पनि काम नगरेकोले सो समितिलाई कार्यान्वयनमा ल्याईनु पर्दछ ।

4.1.2 **वार्षिक तथा रणनैतिक योजना :** कार्यालयले सूचना प्रविधि शाखाको रणनैतिक योजना तथा वार्षिक योजना तयार गरि कार्यान्वयनमा ल्याईनु पर्दछ ।

4.1.3 **सूचना प्रविधि नीति :** कार्यालयमा प्रयोग भएको सफ्टवेयर सुरक्षाको लागि कार्यालयले 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 ।

4.1.4 **तेश्रोपक्ष आश्वस्तता :** तेश्रोपक्ष डिलोइट टच तोमात्सु इण्डिया एलएलपी कम्पनीद्धारा ई-जिपी प्रणालीको पुनरावलोकन पश्चात दिईएका सुझावहरु कार्यालयद्धारा कार्यान्वयन गरिनु पर्दछ ।

4.1.5 **आन्तरीक लेखापरीक्षण :** कार्यालयले आन्तरिक रुपमा प्राविधिक सहितको आन्तरीक लेखापरीक्षण शाखा गठन गरि आन्तरिक लेखापरीक्षण गर्ने व्यवस्था गरिनु पर्दछ ।

4.1.6 **जनशक्ति व्यवस्थापन :** कार्यालयले आवश्यक दरबन्दिको बन्दोवस्त गरि सूचना प्रविधिका नेटवर्क प्रशासक, प्रणाली प्रशासक तथा डाटावेश प्रशासक जस्ता मूख्य कार्यहरुका साथै सफ्टवेयरको परिवर्तनहरु तथा अद्यावधिक जस्ता कार्यहरुमा कार्यालयकै कर्मचारीहरुबाट गराउनु पर्दछ ।

4.1.7 **कर्मचारी तालीम :** कार्यालयले सूचना प्रविधि तालिमको आवश्यकता पहिचान गरी कर्मचारीहरुलाई योजनाबद्ध तालीम दिई बाह्यश्रोत(बाह्य कर्मचारी) माथिको परनिर्भरतालाई न्यून बनाउँदै लैजानु पर्दछ ।

4.1.8 **हेल्पडेस्क :** कार्यालयले लाभग्राहीको समस्या तथा समयमा समाधान गर्न (रियल टाईम ईनसिडेन्ट मनिटोरिङ टुल : सिआईईएम) जस्ता प्रविधि उपयोग गरी चौविसै घण्टा सेवा प्रदान गर्ने तथा घटनाक्रम व्यवस्थापन नीति(इनसिडेन्ट म्यानेजमेण्ट पोलिसी) तयार गरी हेल्पडेस्कलाई जिम्मेवार बनाईनु पर्दछ ।

4.1.9 **नियमितता परीक्षण :** कार्यालयले सञ्जालहरु फायरवालद्धारा ब्लक गरिएको, अवाँछित पोर्टहरु डिसेबल गरिएको, अवाँछित गतिविधिहरुलाई आईपि एर्डस मार्फत ब्लक गरिएको लगायतका कार्य गरी ब्यवस्थित गर्ने प्रयास गरिएको, अन्य नेटवर्कसंग भर्चुअल प्राईभेट नेटवर्क(भिपीएन) मार्फत मात्रै सम्पर्क गर्ने गरिएको र नेटवर्क तथा एप्लिकेशन प्रणालीको अनुगमन परिक्षणका लागि पेनडोरा तथा जिनोस(ओपन सोर्स) औजार प्रयोग गरेको जनाएकोमा आवश्यक नीति तथा मापदण्ड तयार गरी व्यवस्थापनबाट स्वीकृत पश्चात कार्यान्वयन गरिनु पर्दछ ।

4.1.10 **उपयोगकर्ता प्रक्रिया(युजर म्यानूअल/प्रोसिडुअर) :** कार्यालयले यूजर म्यानुअल तयार गरि तथ्यांक तथा सूचनाहरुमा अनधिकृत पहुँच तथा चुहावट नियन्त्रण सहित प्रविधि पहुँचलाई सुरक्षित बनाईनु पर्दछ ।

4.1.11 **पासवर्ड :** कार्यालयले सम्झन सकिने, अक्षर तथा अंकको कम्प्लेक्स वर्ड र निश्चित समयमा अनिवार्य परिवर्तन गर्नुपर्ने व्यवस्था सहितको पासवर्ड नीति स्वीकृत गराई कार्यान्वयन गरिनु पर्दछ ।

4.1.12 **कार्य विभाजन :** कार्यालयले डाटावेश तथा नेर्टवर्क प्रणाली सन्चालनमा एप्लिकेशन यूजरसंग भएको सम्झौतालाई बाद्यकारी कार्यान्वयको व्यवस्था गरी सिस्टम यूजरहरुको काम कर्तव्य अधिकारको स्पष्ट व्यवस्था सहति प्रणाली प्रयोगलाई प्रभावकारी बनाईनु पर्दछ ।

4.1.13 **लग ईन तथा लग आउट :** कार्यालयले लग ईन तथा लग आउट नीतिको तर्जुमा सहित सफ्टवेयरको सुरक्षाको लागि सक्रिन सेभरको समयावधी कम गर्ने तथा सफ्टवेयरमा टेम्पोरोरी सेभ एण्ड नेक्सट वटमको व्यवस्था गर्नुपर्ने देखिन्छ ।

4.1.14 **अडिट लग र अनुगमन :** कार्यालयद्धारा एप्लिकेशन तथा प्रणालीको प्रयोगमा आएका समस्या समाधानका लागि अडिट लग अद्यावधिक गरी नियमित अनुगमन गर्ने व्यवस्था गरिनु पर्दछ ।

4.1.15 **नवप्रवेशी तथा छाडनेहरुको व्यवस्थापन** : कार्यालयले सरुवा भई आउने तथा सरुवा भई जाने सफ्टवेयर प्रयोगकर्ताको यूजर आईडिको निर्माण र प्रोफाईल लक गर्दा प्रणाली मार्फत नै गरिने संयन्त्रको विकास गरिनु पर्दछ ।

4.1.16 **प्रणाली सञ्चालक (सिस्टम एडमिनिस्ट्रेसन)** : प्रणाली सञ्चालक तथा सुपर युजरमा आन्तरिक श्रोतकै कर्मचारीहरुलाई लगाउने तथा सूचना प्रविधि प्रमुखको स्वीकृतमा निश्चित समयको अन्तरालमा प्रणाली सन्चालक परिवर्तन गरि तेश्रोपक्ष माथिको परनिर्भतालाई कम गर्दै लैजानु पर्दछ ।

4.1.17 **एप्लिकेशन नियन्त्रण** : कार्यालयले ई-जिपी प्रणालीको सम्पूर्ण प्रक्रिया स्पष्ट देखिने गरी सिस्टम म्याप तयार गर्नुपर्ने तथा युजर एसप्टेन्स टेस्ट(यूएटी) प्रतिवेदनमा उल्लिखित सुझावहरु कार्यालयद्धारा कार्यान्वयन गरिनु पर्दछ ।

4.1.18 **एन्टिभाइरस** : कार्यालयले ई-जिपी सफ्टवेयर प्रणालीमा अपलोड हुने अभिलेख तथा फायलहरु अनिवार्यरुपमा स्वतः स्क्यान हुने एन्टिभाईरस प्रणाली जडान गरि ई-जिपी प्रणालीलाई सुरक्षित गरिनु पर्दछ ।

4.1.19 **डाटावेश सुरक्षा** : कार्यालयले सफ्टवेयर तथा डाटाको सुरक्षाको लागि (डाटावेश एक्टिभिटी अनुगमन-डिएम) जस्तो नवीन प्रविधिको प्रयोगतर्फ अग्रसर हुनुपर्ने देखिन्छ ।

4.1.20 **पूर्वाधार पहुँच सुरक्षा विधि(फिजिकल एक्सेस सेक्यूरिटि प्रोसिडिअर)** : कार्यालयले सूचना प्रविधिको भौतिक पूर्वाधार सुरक्षाका लागि नीति तथा विधि स्वीकृत गराई कार्यान्वयन ल्याईनु पर्दछ ।

4.1.21 **पूर्वाधार सुरक्षा** : संवेदनशील उपकरणहरु राखिएका सर्भर कक्ष, नेटवर्क स्वीच जस्ता सम्वेदनशील क्षेत्रमा प्रवेशकर्ताहरुको प्रवेश तथा बाहिरिएको अभिलेख स्वचालित रुपमा रही अनुगमन गर्ने तथा अनिवार्य प्रवेशपासको व्यवस्था गरि जोखिम न्यून गरिनु पर्दछ ।

4.1.22 **अनुगमन** : स्वचालित कार्य सञ्चालनमा अनधिकृत फाइल, तथ्यांक वा गल्तिहरुलाई विश्लेषण गरि सफ्टवेयर तथा तथ्यांकहरुबाट हटाउन तथा रोक्नका लागि कार्यालयद्धारा आन्तरिक तथा नियमित रुपमा ई-जिपी सफ्वेयरका विशेष जोखिमहरु मूल्यांकन तथा अनुगमन गरिनु पर्दछ ।

4.1.23 **व्याकअप नीति :** उचित व्याकअप नीति तथा तथ्याङ्क व्याकअपको लागि कार्यालयले योजना एवं सूची तयार गरि नियमित रुपमा पुनःभण्डारण(रिस्टोरिङ्ग)को व्यवस्था गरिनु पर्दछ ।

4.1.24 **तेश्रोपक्ष** : कार्यालयले सहायता कक्ष व्यवस्थापक(हेल्प डेस्क म्यानेजर), प्रणाली व्यवस्थापक (सिस्टम एडमिनिष्ट्रर), नेटवर्क व्यवस्थापक, डाटाबेस व्यवस्थापक(डाटावेश एडमिनिष्ट्रर)को लागि बाह्य श्रोतबाट नियुक्त नगरि आन्तरीक कर्मचारीहरुको क्षमता विकास गरि तेश्रोपक्षमाथिको परनिर्भरता नियन्त्रण गरिनु पर्दछ ।

4.1.25 **ईन्टरफेस** : कार्यालयले शुद्ध एवं सुरक्षित तथ्याङ्क स्थान्तरणका लागि सुरक्षित नेटवर्क तथा निर्देशिका तयार गरि कार्यान्वयन गरिनु पर्दछ ।

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

4.1.27 **सेक्युरिटी लग्स्** : कार्यालयले सूचना प्रविधिको प्रयोगमा आईपरेका सबै किसिमका सुरक्षा चुनौती(सेक्यूरिटि थ्रेट) को अभिलेख तथा सेक्यूरिटि लग्सको व्यवस्था गरी त्यसको उच्च व्यवस्थापन मार्फत विश्लेषण गरि समाधान गर्ने व्यवस्था गरिनु पर्दछ ।

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

4.1.29 **तथ्याङ्क धुल्याउने** : कार्यालयले तथ्याङ्क धुल्याउने प्रगिङ, किलियरिङ्ग जस्ता विभिन्न पद्धति प्रयोग मार्फत जाँच गरी तथ्याङ्कहरु धुल्याएर तथ्याङ्क भण्डारण स्थान(डाटा स्टोरेज स्पेस)को क्षमता बढाइनु पर्दछ ।

4.1.30 **व्यवसाय निरन्तरता योजना र प्रकोप पुनःस्थापना योजना(बीसीपी तथा डीआरपी) :** सूचना प्रविधि प्रणालीको भावी चुनौतीहरुलाई ध्यानमा राखी कार्यालयले व्यवसाय निरन्तरता योजना एवं प्रकोप पुनःस्थापना योजना तयार गरी कार्यान्वयन गरिनु पर्दछ ।

41.31 **केन्द्रीय अभिलेख :** नेपाल सरकारको सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका ,२०७१ मा भएको व्यवस्थाको परिपालना गरी उपयोगमा ल्याईएको सफ्टवेयरहरु सूचना प्रविधि विभागमा अभिलेखकिरण गरिनु पर्दछ ।

41.32 **अनुकुलित/परिमार्जीत सूचना प्रविधि प्रणाली(कस्टुमाईज्ड/बीस्कोप आईटी सिस्टम) :** प्रयोगमा ल्याईएको सूचना प्रविधि प्रणाली(कस्टुमाईज्ड/बीस्कोप आईटी सिस्टम) सम्बन्धमा कार्यालयले नियमित तथा समयानुकुल प्रयोग पश्चात पुनरावलोकन(पोष्ट ईम्प्लिमेन्टेसन रिभ्यु)को व्यवस्था गरिनु पर्दछ ।

41.33 **उच्च व्यवस्थापन स्वीकृती(सिनियर म्यानेजमेन्ट एप्रुभल)** : कार्यालयले स्वचालीत अभिलेखाङ्कन प्रणाली जडान गर्ने, निर्धारित समयमा पुनरावलोकन गर्ने तथा परिमार्जन पूर्व उच्च व्यवस्थापनको स्वीकृति गराउने व्यवस्था मिलाउनु पर्दछ ।

41.34 **कार्य विभाजन :** कार्यालयले सफ्टवेयर प्रणालीको तथ्याङ्कहरुको विकास, परिमार्जन, परिक्षण, कार्यान्वयन र स्थान्तरण(डेभलपमेण्ट, मोडिफिकेशन, टेस्टिङ्ग, डिप्लोएमेण्ट/म्याईग्रेसन) गर्ने कार्य फरक फरक बातावरणमा व्यवस्थित गरिनु पर्दछ ।

41.35 **उपयगोकर्ता स्वीकृति परिक्षण(यूजर एसप्टेन्स टेस्ट) :** कार्यालयले सूचना प्रविधि प्रणालीमा प्रयोग गरिएका सम्पूर्ण परिमार्जनको स्वचालित अभिलेख राख्ने तथा उपयोगकर्ता स्वीकृति परिक्षण पश्चातमात्र उपयोगमा ल्याउने व्यवस्था गरिनु पर्दछ ।

41.36 **परिवर्तन व्यवस्थापन(चेञ्च म्यानेजमेण्ट) :** परिवर्तन व्यवस्थापन(चेञ्च म्यानेजमेण्ट), प्रणाली प्राप्ति(सिस्टम एक्यूजिसन) तथा आकस्मिक प्रणाली परिमार्जन(ईमरजेन्सी सिस्टम मोडिफिकेसन) गर्न कार्यालयले आवश्यक विधि तयार गरि सो अनुसारको अनुसारको प्रक्रिया अवलम्बन गरिनु पर्दछ ।

41.37 **वारेण्टी :** हार्डवेयर तथा सफ्टवेयरको सुरक्षाको लागि कार्यालयले हार्डवेयर तथा सफ्टवेयर प्राप्ति गर्दा निश्चित अवधिको वारेन्टि सहित लागत लाभ विश्लेषण गरिनु पर्दछ ।

41.38 **प्रयोग पश्चात पुनरावलोकन(पोष्ट ईमप्लिमेन्टेसन रिभ्यु)** : कार्यालयमा प्रयोगमा आएको सफ्टेयर प्रणालीको विकास तथा परिमार्जनको एक निश्चित समयमा प्रयोग पश्चातको पुनरावलोकन(पोष्ट ईमप्लिमेन्टेसन रिभ्यु) गरिनु पर्दछ ।

41.39 **प्रणाली प्रयोगको लागि दर्ता** : विद्युतीय खरिद प्रणाली सञ्चालन निर्देशिका, २०७४ को परिच्छेद-३ को दफा ६ र ७ अनुसार सार्वजनिक खरिद अनुगमन कार्यालयले मन्त्रालय विभाग र केन्द्रियस्तरको निकाय दर्ता गर्ने र प्रादेशिक, जिल्ला र स्थानीयस्तरका निकायहरु सम्बन्धित तालुक निकायबाट दर्ता गर्ने व्यवस्थाको पालना गरिनु पर्दछ ।

41.40 **बोलपत्र सूचना प्रकाशन तथा प्रस्ताव दर्ता :** विद्युतिय खरिद प्रणाली सञ्चालन निर्देशिका, २०७४को दफा १३ अनुसार बोलपत्र सूचना प्रकाशन तथा दफा १६ अनुसार बोलपत्रदाताहरुले आफ्नो बोलपत्र प्रस्ताव अनलाईन मार्फत दर्ता गराउने व्यवस्थाको परिपालना गरिनु पर्दछ ।

41.41 **बोलपत्र मूल्याङ्कन,स्वीकृती र भुक्तानी** : विद्युतिय खरिद प्रणाली सञ्चालन निर्देशिका, २०७४ को दफा २२ अनुसार बोलपत्र प्रस्तावको मूल्याङ्कन, दफा २३ अनुसार बोलपत्र स्वीकृतिको आशयको सूचना, पुनरावलोकन तथा बोलपत्र स्वीकृतिको पत्र र दफा २८ अनुसार कामको अग्रिम/पेश्की/रनिङ्ग बिल/अन्तिम बिल/क्षतिपूर्ति लगायतका विलहरु अनलाईन मार्फत पेश गर्ने र भुक्तानी दिनुपर्ने व्यवस्थाको कार्यान्वयन गरिनु पर्दछ ।

41.42 **विद्युतीय खरिद प्रणालीको प्रयोग(ईम्प्लीमेन्टेसन अफ ई-जिपी सिस्टम)** : ई-जिपी प्रणालीको सफल कार्यान्वयनको लागि विद्युतिय खरिद प्रणाली सञ्चालन निर्देशिका, २०७४ मा नै ई-जिपी प्रणालीलाई अनिवार्य प्रयोग गर्ने व्यवस्था गर्ने तथा प्रणाली कार्यान्वयनको अनुगमनलाई प्रभावकारी बनाईनु पर्दछ ।

41.43 **बैंक जमानतको अनुगमन** : विद्युतीय सरकारी खरिद प्रणालीले स्वचालित रुपमा बैंक जमानतको परीक्षण तथा अनुगमन गर्ने संयन्त्रको विकास गरिनु पर्दछ ।

४.२ निष्कर्ष :

सार्वजनिक खरिद अनुगमन कार्यालयले सार्वजनिक खरिद प्रक्रियामा देखिएको अस्वस्थ प्रतिस्पर्धालाई न्यून गरी खरिद प्रक्रियालाई खुल्ला, पारदर्शी, वस्तुनिष्ठ र विश्वसनीय बनाउने उद्देश्यले २०६४।५।३ देखि सिंगल पोर्टलमा आधारित सार्वजनिक विद्युतीय खरिद प्रणालीलाई प्रयोगमा ल्याईएता पनि सार्वजनिक खरिद अनुगमन कार्यालयले प्रयोगमा ल्याएको ई-जिपी सूचना प्रविधि प्रणालीको सुरक्षा सम्बन्धमा हालसम्म सूचना प्रविधि नीति, सूरक्षा नीति, व्यवसाय निरन्तरता नीति, डिजास्टर रिकभरी नीति लगायतका नीतिहरु तयार नगरेको, सेक्युरिटी लगस्को समय समयमा सुपरीवेक्षण हुने नगरेको, प्रयोगमा ल्याएको सूचना प्रविधि प्रणालीहरु सूचना प्रविधि विभागमा अभिलेखीकरण नगरिएको, सूचना प्रविधि प्रणाली प्रयोगमा ल्याउनु पूर्व यूजर एसप्टेन्स टेस्ट नगराएको जस्ता ब्यहोराहरु देखिएकोमा ई-जिपी प्रणालीलाई पूर्णत सूचना प्रविधिमा आधारित बनाउनको लागि उल्लेखित सुधारका उपायहरुलाई अवलम्बन गरिनु पर्दछ ।