नवकान्तिपुर बचत तथा ऋण सहकारी संस्था लि.

बत्तिसपुतली, काठमाण्डौ

सूचना प्रविधि नीति तथा कार्यविधि-२०८१

नवकान्तिपुर बचत तथा ऋण सहकारी संस्था लि.
बत्तिसपुतली, काठमाण्डौ
सूचना प्रविधि नीति तथा कार्यविधि-२०८१

प्रस्तावना : संस्थाको कारोबारको सिलसिलामा समय सापेक्ष प्रविधिको विस्तार गर्दै कारोबारलाई व्यवस्थित, प्रभावकारी र सुरक्षित बनाउन यो सूचना प्रविधि नीति तथा कार्यविधि तयार गरी लागू गरिएको छः

१. **नाम :** यस नीतिको नाम 'सूचना प्रविधि नीति तथा कार्यविधि-२०८१' हुनेछ ।

२. **प्रारम्भ :** यो नीति संस्थाको बार्षिक साधारण सभाबाट पारित भएको मितिदेखि लागु हुनेछ ।

३. **परिभाषा :** विषय वा प्रसङ्गले अर्को अर्थ नलागेमा यस नीति तथा कार्यविधिमा :

३.१ "संस्था" भन्नाले नवकान्तिपुर बचत तथा ऋण सहकारी संस्था लिमिटेड, बत्तिसपुतलीलाई सम्झनु पर्नेछ ।

३.२ "सदस्य" भन्नाले तोकिएको प्रक्रिया पुरा गरी संस्थाको सदस्यता लिएको व्यक्ति वा संस्थालाई सम्झनु पर्नेछ ।

३.३ "कर्मचारी" भन्नाले तोकिएको प्रक्रिया पुरा गरी संस्थामा नियुक्ति पाएका स्थायी, अस्थायी, करार र ज्यालादारी कर्मचारीलाई सम्झनु पर्नेछ ।

४. सूचना तथा प्रविधिको प्रयोगः

४.१ संस्थाको कारोबारको सिलसिलामा प्रमुख कार्यकारी/महाप्रवन्धकको मातहतमा रहने गरी छुट्टै सूचना तथा प्रविधि (आइटी) विभाग रहने छ ।

४.२ संस्थासँग सम्बन्धित सम्पूर्ण कारोबारलाई कम्प्युटर प्रविधिको प्रयोग गरी सुरक्षित र सहज बनाइने छ ।

४.३ संस्थाको नाममा वेभसाइट, सदस्य भाईवर ग्रुप र फेसबुक पेज निर्माण गरी सो मार्फत संस्थाका गतिविधिहरू सार्वजनिक गरिनेछ ।

४.४ संस्था अन्तर्गतका कार्यालयगत कारोबारलाई अन्तरकार्यालय सञ्जाल (Networking) मार्फत केन्द्रिकृत गरिने छ ।

४.५ सूचना प्रविधिको क्षेत्रमा भएका र भविष्यमा हुने विकासलाई संस्थाको आवश्यकताका आधारमा क्रमशः आत्मसाथ गर्दै लगिने छ ।

४.६ कार्यालयहरुमा रहेका कम्प्युटरमा अफिसियल सफ्टवेयर जडान संस्थाको आइटी विभाग मार्फत हुनेछ । अनधिकृत सफ्टवेयर, प्रोग्राम जडान गर्न पाइने छैन ।

४.७ सेवा प्रदायक निकायको सहयोगमा कम्प्युटर, सफ्टवेयर तथा अन्य सूचना प्रविधि सम्बन्धि उपकरणहरु समय-समयमा अद्यावधिक तथा मर्मत सम्भार गरिने छ ।

४.८ डिजिटल कारोवार प्रणालीको व्यवस्थापनको लागि संस्थाको केन्द्रिय कार्यालयमा डिजिटल कारोवार प्रमुखको नेतृत्वमा एक डिजिटल कारोवार विभागको स्थापना गरिनेछ ।

५. डाटा सेन्टर व्यवस्थापन (Data Centre Management) :

५.१ आइटी विभागको जिम्मेवारीमा संस्थाको प्रधान कार्यालयमा डाटा सेन्टर रहनेछ ।

५.२ उक्त डाटा सेन्टरमा Computer Servers, Networking Equipments, Switch, Firewall Device, Router, UPS तथा सूचना प्रविधिसँग सम्बन्धित महत्वपूर्ण उपकरणहरु रहनेछन् ।

५.३ Data Centre मा अनधिकृत व्यक्तिलाई प्रवेश निषेध हुनेछ । प्रमुख कार्यकारी/महाप्रवन्धक, आइटी विभाग प्रमुख वा निजले तोकेको व्यक्ति मात्र यस सेन्टरमा प्रवेश गर्न सक्नेछन् ।

५.४ डाटा सेन्टरमा कुनै पनि खानपानका वस्तुहरु, प्रज्वलनशिल पदार्थहरु लैजान पाइने छैन ।

५.५ डाटा सेन्टरमा उपयुक्त तापक्रम कायम राख्नु पर्नेछ ।

५.६ डाटा सेन्टरमा प्रवेश गर्दा र बाहिरिँदा अनिवार्य लगबुक भर्नुपर्नेछ ।

५.७ डाटा सेन्टरको सुरक्षा गर्ने जिम्मेवारी सम्बन्धित विभागीय प्रमुख र तोकिएको कर्मचारीको हुनेछ ।

६. सेवा प्रणाली व्यवस्थापन (Server System Management) :

संस्थाबाट प्रदान गरिने सेवालाई प्रभावकारी र सुरक्षित बनाउन प्रधान कार्यालय बत्तिसपुतलीमा निम्नअनुसार सेवा प्रणाली स्थापना गरी सोको व्यवस्थापन गरिने छ :

६.१ तथ्याङ्कमा आधारित सेवा (Database Server- Mainserver) :

६.१.१ मेनसर्भर नामक यो सर्भरबाट संस्थाको सम्पूर्ण तथ्यांक सुरक्षित गरिने छ ।

६.१.२ यो सर्भरलाई २४ सै घन्टा लाइभ सर्भरको को रुपमा प्रयोग गरिने छ ।

६.१.३ यो सर्भरले रिमोट टेलर सञ्चालन कार्य गर्ने छ ।

६.१.४ यो सर्भरले संस्थाको सफ्टवेयरसँग सम्बन्धित सम्पूर्ण डाटा स्टोर गर्ने छ ।

६.२ प्रतिलिपि सेवा (Back-up Server- Indrachwok) :

६.४.१ ईन्द्रचोक नामक यो सर्भरमा पुरानो Datebase सुरक्षित गरिने छ ।

६.४.२ यो सर्भरलाई विशेष अवस्थामा अस्थायी रुपमा अन्य सर्भरको उद्धारकर्ता सर्भरको रुपमा प्रयोग गरिने छ ।

६.३ डाटा ब्याकअप (Data Backup) :

६.३.१ संस्थाले प्रयोगमा ल्याएको बैकिङ्ग सफ्टवेयरसँग सम्वन्धित अघिल्लो दिनको डाटाहरुलाई आइटी विभागमार्फत् यस सर्भर कम्प्युटरमा ब्याकअप गरिनेछ ।

६.३.२ यस सर्भरलाई प्रधान कर्यालय स्थित आइटि विभागमा ब्यवस्थित पुर्वाधार सहित ब्यवस्थापन गरिनेछ ।

६.३.३ केन्द्रिय सर्भरवाट डाटा ब्याकअप कार्यालय समय बाहेकको समयमा लिनुपर्नेछ ।

६.३.४ संस्थाको डाटा सुरक्षार्थ कारोवारिक तथ्यांक (Data) लाई क्लाउडमा राखि जोखिम न्युनिकरण गर्न सकिनेछ ।

६.३.५ निक्षेप खाताको हस्ताक्षर नमुना कार्ड, सदस्यको नागरिकताको सक्कलको स्क्यान कपी, सदस्यको फोटो लगायतका कागजातहरु आइटी विभागले तोकेको सर्भर लोकेसन तथा छुट्टै हार्डडिक्समा दैनिक ब्याकअप सम्बन्धित कार्यालयले गर्नुपर्नेछ ।

७. नेटवर्क प्रणाली (Network System):

संस्थाको कारोबारलाई एक अर्का कम्प्युटरबिच सञ्जाल निर्माण गर्नका लागि निम्नअनुसार नेटवर्क प्रयोग गरिने छ :

७.१ आन्तरिक नेटवर्क (LAN) : संस्थाका कुनै पनि कार्यालयमा प्रत्येक कम्प्युटरलाई स्विच हबमार्फत इन्टरनल नेटवर्क वायरबाट सम्पर्क गराइने छ ।

७.२ तारराहित नेटवर्क (WAN) :

७.२.१ तारराहित आन्तरिक सञ्जालको माध्यमबाट संस्थाका विभिन्न कार्यालयबिच केन्द्रीय सञ्जालसँग सम्पर्क गराइने छ ।

७.३ फाइबर कनेक्टिभिटी : संस्थाले अन्तर कार्यालय नेटवर्किङ्ग गर्न फाइवर प्रणाली जडान गरिनेछ । जस अन्तरगत कार्यालय सम्पर्क स्थापित गर्न भिपिएन राउटर डिभाइस जडान गरिनेछ ।

७.४ मेनेजेरियल स्चीच : संस्थाको इन्टरनेट दुरुपयोग रोक्न र कम्प्युटरमा भाइरस प्रवेश रोक्न Firewall Managerial Switch लगायतका डिभाइस प्रयोग गरिनेछ ।

८. इन्टरकम कम्युनिकेसन (EPABX) :

संस्थाका सबै कार्यालयहरुमा इन्टरकम कम्युनिकेसन व्यवस्था गरिनेछ ।

९. ई-हाजिरीः

संस्थामा कार्यरत कर्मचारीको हाजिरी व्यवस्थापनलाई चुस्त, दुरुस्त र आधुनिकीकरण गर्न ई-हाजिरी प्रविधि रहनेछ । उक्त प्रयोजनका लागि ई-हाजिरी सफ्टवेयर र थम्प मेशिनको प्रयोग गरिनेछ ।

१०. बैङ्किङ सफ्टवेयरः

१०.१ सफ्टवेयर : संस्थाको कारोबारलाई व्यवस्थित, सहज र प्रभावकारी बनाउन आधिकारिक र अनुभवी सेवाप्रदायक संग कोर बैङ्किङ सिस्टम (Core Banking System) वा सहकारी सफ्टवेयर एप्लिकेशन खरिद गरि प्रयोग गरिने छ । यो एप्लिकेसनका विशेष प्रकारका विशेषताहरु हुनेछन् :

(i) Multiple Branch Banking

(ii) SMS Banking

(iii) Mobile Banking

(iv) Depositary Management

(v) Transaction Verification

१०.२ सफ्टवेयर सम्वन्धि ब्यवस्था :

१०.२.१ संस्थाले सञ्चालनमा ल्याएको सफ्टवेयरमा एकपटक प्रविष्टिगरिएको डिपोजिट एकान्उट, सेयर एकाउन्ट, कर्जा एकाउन्ट, मेम्मर आइडी, जेनेरल लेजरलाई सम्पादन गर्न पाइने छैन । विशेष अवस्थामा भुलबस गरिएको प्रविष्टि सम्पादन गर्नको लागि आइटी विभागको अनुमति अनिवार्य हुनेछ ।

१०.२.२ कुनै बचत खाताको कुनै वा सबै पे अर्डर स्लिप ब्लक गर्न अनुरोध भएमा वा निक्षेप खाता सस्पेन्स गर्नुपर्ने भएमा सो को जानकारी पाउनासाथ सम्बन्धित विभागले गर्नेछ ।

१०.२.३ प्रत्येक कार्यालयले दैनिक सफ्टवेयर सम्बन्धी कारोबारलाई साँझ ८ बजेभित्रमा सम्पन्न गरि सक्नुपर्नेछ । यदि कारणबस कार्य सम्पन्न गर्न नसकिने अवस्था सिर्जना भएमा सम्वन्धित विभागमा अग्रिम जानकारी सहितको निवेदन पेस गर्नुपर्नेछ ।

१०.२.४ त्रैमासिक भौचर एडजसमेण्ट त्रैमासिक अवधि समाप्त भएको ७ दिन र वार्षिक क्लोजिङ भौचर एड्जसमेन्ट आर्थिक वर्ष समाप्त भएको १६ दिन भित्र गरिसक्नुपर्ने छ ।

१०.३ सफ्टवेयरका विशेषता :

१०.३.१ अन्तर कार्यालय आइबिटि गर्न सकिने

१०.३.२ अन्तर कार्यलय बचत खातामा रहेको रकम हेर्न सकिने

१०.३.३ डाटाबेस सफ्टवेयर

१०.३.४ अन्तर कार्यालय भुक्तानीपुर्जा उपलब्ध हुने

१०.३.५ मल्टिपल हस्ताक्षर

१०.३.६ सिंगल डाटाबेस मल्टिपल ब्रान्च

१०.३.७ डिपोजिटरी पर्मिसन

१०.३.८ युजर मेनेजमेन्ट

१०.३.९ मेनु पोलिसी

१०.३.१० भौचर भेरिफिकेसन

१०.३.११ कर्पोरेट रिर्पोट

१०.३.१२ बर्थ डे फिचर

१०.३.१३ इन्स्योरेन्स फिचर

१०.४ मोबाइल स्मार्ट कलेक्सन सम्बन्धि व्यवस्था :

१०.४.१ संस्थाले डिजिटल प्रविधिको प्रयोग गरी बजार प्रतिनिधिहरुमार्फत क्रमशः मोबाइल स्मार्ट कलेक्सन गर्दै लाने छ ।

१०.४.२ एनड्रोइड ओएस भएका स्मार्ट फोनमा संस्थाको कलेक्सन एप्स राखिनेछ ।

१०.४.३ बजार प्रतिनिधिले दिनभरिको कारोबारलाई उक्त एप्समा प्रविष्टि गरी कार्यालयमा ल्याउनु पर्नेछ ।

१०.४.४ कार्यालयले उक्त रेकर्डलाई नगदसँग भेरिफाई गरी सफ्टवेयरम प्रविष्टि गरिने छ ।

१०.४.५ सम्बन्धित बजार प्रतिनिधिले आफूले कलेक्सन गरेको विवरणको एक प्रति प्रिन्ट गरी संस्थाको डिजिटल कारोवार विभाग प्रमुख लाई रुजु गराई कार्यालयमा सुरक्षित राख्नु पर्नेछ ।

१०.५ एसएमएस सर्भिस व्यवस्था :

संस्थाले आफ्ना सेयर सदस्यहरुलाई संस्थागत सूचना सम्प्रेषण गर्न एसएमएस सेवा सञ्चालन गर्न सक्नेछ ।

१०.६. मोवाईल सहकारीता सम्बन्धी व्यवस्था :

१०.६.१ संस्थाले आफ्ना सेयर सदस्यहरुलाई मोवाईल सहकारीता सेवा प्रदान गर्ने छ ।

१०.६.२ सदस्यले आफ्नो मोवाइलमा संस्थाको एप्स मार्फत Fund Transfer गर्न, NTC, Ncell, Internet, Telephone, Dishhome रिचार्ज जस्ता Utility payment सुविधाहरु प्राप्त गर्न सक्नेछन् ।

१०.६.३ माथि उल्लिखित सुविधाका अतिरिक्त सेयर सदस्यलाई आफ्नो खाताको ब्यालेन्स इन्क्वेरी, एकाउण्ड स्टेटमेन्ट, निक्षेप जम्मा तथा फिर्ता गर्दाको नोटिफिकेसन लगायतका सुविधा प्रदान गरिनेछ ।

१०.६.४ माथि उल्लिखित सेवा प्रदान गरेवापत सदस्यले तोकिएबमोजिमको बार्षिक सेवा शुल्क बुझाउनुपर्नेछ । सो रकम सम्वन्धित सदस्यको खातावाट काटिनेछ ।

११. इन्टरनेट प्रयोग :

संस्थाको तर्फबाट इन्टरनेट प्रदायक संस्था (ISP) सँग सम्झौता गरी Unlimited Dedicated Internet प्रयोगमा ल्याइने छ । उक्त इन्टरनेटलाई संस्थाको तारररहित आन्तरिक नेटवर्क (WAN)/फाइबर अप्टीकल मार्फत सबै कार्यालयमा वितरण गरिनेछ ।

१२. ऊर्जा व्यवस्थापन :

संस्थामा जडान गरिएका यन्त्र उपकरण प्रयोगका लागि विद्युत ऊर्जाको विकल्पका रुपमा युपिएस सिस्टम प्रयोगमा ल्याइने छ । साथै आवश्यकता अनुसार जेनेरेटर वा सोलार जडान गरी वैकल्पिक ऊर्जाको रुपमा प्रयोगमा ल्याइनेछ ।

१३. यन्त्र उपकरणहरु :

संस्थाको आवश्यकताका आधारमा विभिन्न कार्यालयहरुमा निम्न यन्त्र उपकरणहरु प्रयोगमा ल्याउँदै लगिने छ :

१३.१ कम्प्युटर सेट

१३.२ विभिन्न प्रकारका प्रिन्टरहरु (लेजर, इन्कजेट, डट आदि)

१३.३ स्क्यानर

१३.४ डिजिटल क्यामेरा

१३.५ नोट काउन्टिङ मेसिन (लुज र बन्डल)

१३.६ फोटोकपी मेसिन

१३.७ प्रोजेक्टर

१३.८ मेटल डिटेक्टर

१३.९ अग्नि नियन्त्रक

१३.१० फेक नोट डिटेक्टर

१३.११ टेलिभिजन

१३.१२ सिसी क्यामेरा रेकर्डर

१३.१३ सिसी क्यामेरा

१३.१४ इकेक्ट्रोनिक्स एटेन्डेन्स

१३.१५ राउटर

१४. वेभसाइट, इमेल र फेसबुकको प्रयोग :

१४.१ संस्थाका विभिन्न गतिविधिहरुलाई इन्टरनेटमार्फत संसारभरि हेर्न र सुन्नका लागि संस्थाको आधिकारिक वेभसाइटको रुपमा www.nawakantipur.com.np रहने छ ।

१४.२ संस्थाको प्रधान कार्यालयको आधिकारिक इमेल ठेगानाको रुपमा info@nawakantipur.com.np रहनेछ ।

१४.३ फेसबुक ठेगानाको रुपमा www.facebook.com/NawakantipurLTD रहने छ ।

१४.४ अन्य कार्यालय तथा निकायको इमेल तपसिल अनुसारको रहनेछ ।

Email
admin@nawakantipur.com.np

battisputali@nawakantipur.com.np

indrachowk@nawakantipur.com.np

account@nawakantipur.com.np

loan@nawakantipur.com.np

cash@nawakantipur.com.np

marketing@nawakantipur.com.np

shiva.sitaula@nawakantipur.com.np

mukunda.pandey@nawakantipur.com.np

haripanday@nawakantipur.com.np

manojsedhai@nawakantipur.com.np

khilanath.ghimire@nawakantipur.com.np

bhola.panday@nawakantipur.com.np

narayanbabu.kandel@nawakantipur.com.np

nawaraj.tripathi@nawakantipur.com.np

binod.sapkota@nawakantipur.com.np

bikash.dulal@nawakantipur.com.np

binod.sedhai@nawakantipur.com.np

sushila.pandey@nawakantipur.com.np

sarita.maharjan@nawakantipur.com.np

sanjita.mainali@nawakantipur.com.np

sushan.maharjan@nawakantipur.com.np

januka.sedhai@nawakantipur.com.np

sharmila.panday@nawakantipur.com.np

१४.५ डोमेन सहितको इमेल व्यवस्थापन :

१४.५.१ संस्थाका कार्यालय प्रमुख तथा विभागीय प्रमुख कर्मचारीहरुलाई कार्यालयको डोमेन नाम राखी इमेल एकाउण्ट प्रदान गरिनेछ आवश्यकताका आधारमा अन्य समिति पदाधिकारी तथा कर्मचारीलाई उक्त इमेल एकाउन्ट उपलब्ध गराउन सकिनेछ ।

१४.५.२ १४.५.१ बमोजिम अफिसियल डोमेन नामको इमेल भएका कर्मचारी संस्थाको सेवाबाट अवकास लिएमा तत्काल त्यस्तो एकाउण्ट खारेज गरिनेछ ।

१४.५.३ यसरी इमेलबाट भएको पत्राचार सार्वजनिक कागजपत्र (Public Document) को रुपमा कार्यालयमा अभिलेख रहनेछ । तर नीजि प्रयोजनमा भएको पत्राचारलाई संस्थागत रुपमा लिइने छैन ।

१४.५.४ अफिसियल डोमेन नामबाट इमेल गरिएका पत्राचारमा व्यक्तिगत गोपनियता (Right of Privacy) लागु हुने छैन ।

१४.५.५ संस्थाले आवश्यक ठानेको बखत त्यस्तो इमेलबाट भएको पत्राचार माथि छानबिन गर्न सक्नेछ ।

१४.६ संस्थाद्वारा जारी परिपत्र, संस्थाको सम्पत्तिका प्रमाणहरु, दर्ता प्रमाणपत्रहरु, संस्था सम्मानित भएका प्रमाणपत्रहरु, प्रत्येक बर्षका अन्तिम लेखापरीक्षण प्रतिवेदन, प्रत्येक बर्षका साधारणसभाको प्रतिवेदन तथा निर्णय, सञ्चालक समितिको बैठकका माइन्यूट, प्रत्येक बर्षका संशोधित नीति तथा कार्यविधि तथा तोकेका अन्य महत्वपूर्ण कागजातहरुको पिडिएफ वा जेपिइजी कपी नियमित रुपमा ब्याकअप गरिनेछ ।

१५. सञ्चार माध्यमको प्रयोग :

संस्थाको कारोबार र गतिविधिसँग सम्बन्धित विभिन्न तथ्यांक र सूचनाहरुलाई प्रत्येक कार्यालयमा रहेको सूचना पाटी, फेसबुक पेज, भाईवर ग्रुप मार्फत सार्वजनिक गरिने छ ।

१६. नवकान्तिपुर स्मार्ट एप्स :

संस्थाका सदस्यहरुको बचत तथा भुक्तानी कारोवार लाई सदस्यकै मोवाईल मार्फत डिजिटल माध्यमबाट गर्नको निमित्त नवकान्तिपर स्मार्ट एप सञ्चालन गरिनेछ ।

१७. संस्थाको वेभसाईट, एप्लिकेशन, सर्भर, स्टोरेज तथा नेटवर्क सुरक्षा सम्बन्धी :

१. संस्थाले प्रयोग गरिरहेको कोर बैंकिङ्ग सफ्टवेयरको दैनिक डाटाबेसलाई प्रधान कार्यालयमा रहेको सर्भरका अतिरिक्त शाखा कार्यालयमा तोकिएको स्थानमा दैनिक रुपमा डाटाबेस ब्याकअप गरिनेछ ।

२. कार्यालयका कम्प्यूटरहरुमा आवश्यक USB पोर्टहरुमात्र Enable गरिनेछ । कार्यालयद्धारा प्रदान गरिएका वा स्वीकृत Removable उपकरणहरुमात्र कम्प्यूटरमा जोड्न मिल्ने गरि सूरक्षा व्यवस्था मिलाईनेछ ।

३. महत्वपूर्ण डाटा र सेवाहरुसँग सम्बन्धित सर्भर र अन्य नेटवर्क उपकरणहरुलाई सुरक्षित बनाउन Network Segmentation लागु गरिनेछ ।

४. Website तथा Application हरुमा अनिवार्य रुपमा SSL Certificate Install गर्ने व्यवस्था मिलाईनेछ ।

५. संवेदनशील सूचना रहने क्षेत्र (Datacenter/Server Room) हरुमा अनाधिकृत पहुँच हुन नदिनको लागि Access Control/Door Luck System को व्यवस्था मिलाईनेछ ।

६. भौतिक सूरक्षाको लागि IP Camera सहितको Surveillance प्रणालीको जडान गरि अनुगमनको व्यवस्था मिलाईनेछ ।

७. Password राख्दा सहजै अनुमान गर्न नसकिने गरि सुरक्षित Password राखिनेछ । Password हरेक तीन तीन महिनामा अनिवार्य परिवर्तन गर्नुपर्ने व्यवस्था मिलाईनेछ ।

८. ईमेल सुरक्षाको लागि Email Service Provider ले प्रदान गरेको Security Features लाई Enable गर्ने व्यवस्था गरिनेछ ।

९. सम्बन्धित कर्मचारीहरुले आफ्नो निकायमा प्रयोग भईरहेका Email लगायतका सूचना प्रविधी प्रणालीहरुमा Multi-factor Authencation को प्रयोगलाई प्रोत्साहन गरिनेछ ।

१०. सूचना प्रविधि सम्बन्धी कार्य गर्ने सम्बन्धित कर्मचारीहरुको लागि नियमित रुपमा Data/Application/Network/Cloud Security लगायतका साईबर सुरक्षा सम्बन्धी तालिम प्रदान गर्ने व्यवस्था मिलाईनेछ ।

१८. कार्यालयमा रहेका डेस्कटप/ल्यापटप र प्रिन्टर सुरक्षा सम्बन्धी :

१. कार्यालयमा रहेका डेस्कटप/ल्यापटप प्रयोग गर्नु नपर्ने अवस्थामा सँधै Lock/Logoff गर्ने तथा कार्यालय छोड्दा डेस्कटप/ल्यापटप लगायतका उपकरणहरुलाई अनिवार्य बन्द गर्ने व्यवस्था मिलाईनेछ ।

२. डेस्कटप/ल्यापटप आवश्यक पर्दा बाहेक GPS,Bluetooth, NFC र अन्य Sensor हरुलाई Disable राख्ने व्यवस्था मिलाईनेछ ।

३. डेस्कटप/ल्यापटपमा Antivirus Client Install गरी सो लाई सबैभन्दा नयाँ Virus Definition, Signature र Pacch हरुमा Upgrade गर्ने व्यवस्था मिलाईनेछ ।

४. USB, External Harddisk लगायतका Plug and Play Devices हरुको प्रयोग गर्दा हरेक पटक Security Scan गरि सुरक्षित रहेको एकिन गरेर मात्र प्रयोग गर्ने व्यवस्था गरिनेछ ।

५. Password, IP Address, Network Diagram वा अन्य संवेदनशील जानकारीलाई सम्बन्धित व्यक्ति बाहेक अरुले नदेख्ने/नभेट्ने ठाँउमा राख्ने व्यवस्था मिलाईनेछ ।

६. अति आवश्यक परेको बेलामा मात्र सीमित समय र सीमित प्रयोगकर्ताका लागि मात्र File/Folder Sharing गर्ने व्यवस्था मिलाईनेछ ।

१९. कार्यालयको ईमेल तथा Phishing Attack सुरक्षा सम्बन्धी :

१. अपरिचित व्यक्ति तथा संस्थाबाट आएका Email हरु Phishing तथा Spam Email हुन सक्ने हुँदा त्यसको आधिकारिकता पुष्टि नभएसम्म नखोल्ने व्यवस्था मिलाईनेछ ।

२. अपरिचित व्यक्ति वा ठेगानाबाट आएको शंकास्पद ईमेलको File/Photo/Link लाई नखोल्न र तत्काल Delete गर्न, अत्यावश्यक बाहेकका Webpage/Newsletter/Mailing List हरुमा Subscribe नगर्न, ईमेल SMS वा फोन मार्फत आफ्नो Password, OTP, Bank Account Number, PIN Code जस्ता विवरणहरु नपठाउन सम्बन्धित कर्मचारीहरुलाई सूसुचित गरिनेछ ।

३. ईमेल खातामा Multi-Factor Authentication लाई Enable गर्ने व्यवस्था गरिनेछ ।

२०. सम्पत्ति सामानको वारेण्टी कार्ड व्यवस्थापन :

संस्थाले खरिद गरेको सम्पत्ति सामानको वारेन्टी कार्ड सुरक्षित राख्ने गरि कार्यालयमा वारेन्टी कार्ड फायल खडा गरी सुरक्षित गरिनेछ । यसरी सुरक्षित गरिएको वारेन्टी कार्ड लामो समयसम्म वारेन्टी पाइने ब्याट्री लगायत खराब भएको अवस्थामा सेवा प्रदायक कम्पनीले वारेन्टी माग गर्दा सो कागजात उपलब्ध गराउनुपर्ने भएको अवस्थामा सम्बन्धित कार्यालयले प्रधान कार्यालयलाई उपलब्ध गराउनुपर्नेछ । वारेण्टि कार्ड उपलब्ध नभएको अवस्थामा सम्वन्धित कार्यालयका प्रमुखले सो को दायित्व वहन गर्नुपर्नेछ ।

२१. कम्प्युटर सफ्टवेयरको व्यवस्था :

संस्थाले आफ्नो कार्यालयमा प्रयोग गरेको कम्प्युटर सिस्टममा संस्थाको आवश्यकतासँग सम्वन्धित रहेर तोकेको विन्डोज तथा एप्लीकेसन सफट्वेयर मात्र प्रयोग गर्नु पर्नेछ । विभिन्न प्रकृतिका सफ्टवेयर इन्स्टल गर्दा संस्थालाई हानि नोक्सानी पुर्याउने हुँदा सफट्वेयर प्रयोग निषेध गरिनेछ । अनाधिकृत सफ्टवेयर इन्स्टल गरि प्रयोग गर्दा भाईरस संक्रमण हुने, नेटवर्किङ्ग सिष्टममा असर पुग्ने, कामकाजमा एकरुपताको समस्या सृजना हुने हुँदा जानजानी त्यसो गरेको खण्डमा संस्थाको मानव संसाधन निति तथा कार्यविधि अनुसार दण्ड सजायको भागीदार बन्ने व्यवस्था गरिनेछ ।

२२. कम्प्युटर सञ्चालन :

संस्थाको सम्पुर्ण कम्प्युटर सिस्टमलाई अनिवार्यरुपमा डोमेनमा राखिनेछ र प्रयोगकर्तालाई डोमेन युजरनेम र पासवर्ड प्रदान गरिनेछ । कम्प्युटरको सुरक्षा गर्नु सम्वन्धित कर्मचारीको दायित्व हुनेछ । साथै कम्प्युटर खराव हुन नदिन सचेत रहनु पर्नेछ । कम्प्युटरमा कुनै खरावी देखिएमा आईटि विभागमा समस्याको जानकारी गराउनुपर्नेछ । मर्मत सम्भारको आवश्यकता

परेमा सम्वन्धित कार्यालयमार्फत सिफारिस गरि केन्द्रिय कार्यालयमा पठाउने र केन्द्रिय कार्यालय मार्फत स्वीकृत पश्चात मर्मत सम्भारको प्रकृया पुरा गर्न सकिनेछ ।

२३. यन्त्र उपकरण व्यवस्थापन :

प्रधान कार्यालयको स्वीकृति विना आन्तरिक तथा बाह्य नेटवर्क विस्तार गर्न, टेलिफोन एस्कटेन्सन राख्न, सिसि क्यामेराको लोकेसन परिवर्तन तथा थप गर्न, इ एटेन्डेन्सको स्थान परिवर्तन गर्न, स्वीच, राउटर प्रयोग गर्न वायरलेस डिभाईस तथा ल्यान स्वीच राख्न, कम्प्युटरमा मोवाईल जोड्ने, ल्यापटपमा हटस्पोट बनाउने, भाईरस संक्रमण भएको पेन ड्राइभ प्रयोग गर्ने जस्ता कार्य गर्दा नेटवर्किङ्ग सिष्टममा असर पर्ने हुँदा त्यसो गर्न निषेध गरिएको छ । साथै कार्यालयमा एकपटक सेटअफ गरि निश्चित स्थानमा ब्यवस्थित गरिएको यन्त्र उपकरणलाई सूचना प्रविधी विभागको परामर्शमा मात्र उपयुक्त ठहरेबमोजिम स्थान परिवर्तन गर्न सकिनेछ ।

२४. आइटी कक्षको व्यवस्था :

संस्थाका प्रत्येक कार्यालयमा कार्यरत कर्मचारीमध्ये सम्बन्धित कार्यालय प्रमुखको सिफारिसमा आइटी विभागको तर्फबाट आइटी हेर्ने जिम्मेवारी प्रदान गरिने छ । उक्त जिम्मेवारी प्राप्त गर्ने कर्मचारीले विभागको सहयोगमा आफ्नो कार्यालयमा उत्पन्न हुने आइटीसँग सम्बन्धित समस्या समाधान गर्नु पर्नेछ ।

२५. सर्भर कक्षको व्यवस्था :

संस्थाको सर्भर कक्षहरुलाई पुर्णत ब्यवस्थित गरिनेछ । सर्भर कक्षमा आधिकारिक व्यक्ति वा कार्यालय प्रमुखको अनुमति लिएर मात्र प्रवेश गर्नुपर्नेछ । प्राविधिक फाँटको जिम्मेवारी प्राप्त कर्मचारी वा कार्यलय प्रमुखले सर्भर कक्षलाई जोखिममुक्त राख्नु पर्नेछ ।

२६. पावर ब्याकअपको व्यवस्था :Powerbakup :

संस्थाले विभिन्न कार्यालयहरुमा आवश्यकता अनुसार अनलाईन, युपियस, इन्भर्टर प्रयोगमा ल्याउनेछ । दैनिक कारोबारको लागि अत्यावश्यक उपकरण मात्र प्रयोग गरिनेछ । कम्प्युटर, प्रिन्टर र अत्यावश्यक उपकरण वाहेकमा बढी लोड लिने फोटोकपि मेसिन, फ्रिज, एसी, फेन, कुलर, हेभी प्रिन्टर तथा अन्य बढि क्षमताको लोड लिने यन्त्र उपकरण जडान गरिनेछैन । निषेधित गरिएका यन्त्र उपकरण प्रयोगबाट समस्या सिर्जना भए सम्बन्धित कर्मचारी जवाफदेही हुने व्यवस्था गरिनेछ ।

२७. जेनेरेटर व्यवस्थापन :

संस्थाले आफ्नो कार्यालयहरुमा आवश्यकता अनुसारको जेनेरेटर प्रयोगमा ल्याउनेछ । जसले लाइन नभएको अवस्थामा फोन, फोटोकपि मेसिन सञ्चालन गर्न र इन्र्भटर, युपियस, अनलाईन सिष्टम चार्जिङ्ग गर्न मद्दत पुर्‍याउनेछ ।

२८. प्राविधिक जनशक्ति व्यवस्था :

संस्थाले सूचना तथा प्रविधि विभागको गठनसँगै कार्यालयगत रुपमा संस्थालाई आवश्यक पर्ने प्राविधिकरुपमा विषयगत ज्ञान भएका दक्ष, क्षमता र योग्यता पुगेका जनशक्ति व्यवस्थापन गर्नेछ ।

२९. व्याख्या गर्ने अधिकार :

यो नीति तथा कार्यविधिको व्याख्या गर्ने अधिकार सञ्चालक समितिमा निहित रहने छ ।

३०. संशोधन :

यो नीति तथा कार्यविधिको कुनै पनि बुँदामा संशोधन, खारेज वा थप गर्ने अधिकार सञ्चालक समितिको सिफारिसमा साधारण सभाले गर्नेछ ।

३१. बचाउ :

यो नीति तथा कार्यविधि जारी हुनुपूर्व संस्थामा भएगरेका सूचना प्रविधिसंग सम्बन्धित सम्पूर्ण कार्यहरू यसै नीति तथा कार्यविधि बमोजिम भए गरेको मानिने छ ।

॥ समाप्त ॥

संस्थाको २७औं बार्षिक साधारण सभाबाट पारित
मिति २०८१ साल पौष २० गते शनिवार