नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

प.सं. ०८१/८०
च.नं. ७४

सिंहदरबार, काठमाडौं

मिति : २०८०/०१/०४

विषयः सुझाव उपलब्ध गराउनु हुन अनुरोध ।

उपरोक्त सम्वन्धमा यस मन्त्रालयबाट तयार पारिएको राष्ट्रिय साइबर सुरक्षा नीति, २०८० को मस्यौदा यसै पत्रसाथ सार्वजनिक गरिएको छ। नीति मस्यौदामा कुनै सुझाव भए सात (७) दिन भित्र उपलव्ध गराइदिनु हुन सम्बन्धित सबैमा सादर अनुरोध गर्दछु ।

सुझाब उपलव्ध गराउने इमेल ठेगाना :

१. info@mocit.gov.np

२. *tanka.mahat@nepal.gov.np*

(टंकबहादुर महत)
उपसचिव (कानून)

फोन नं. : ४२११५५६, ४२११६५०, ४२११६१५, फ्याक्स नं.: ४२११७२९, ४२११६१०
Email : info@mocit.gov.np, Website: www.mocit.gov.np

राष्ट्रिय साइबर सुरक्षा नीति, २०८०

१. पृष्ठभूमिः

सूचना प्रविधिमा भएको तीव्र विकाससँगै सामाजिक अन्तरक्रिया, सार्वजनिक सेवा एवम् सूचना प्रवाहमा आमूल परिवर्तन भएको छ। सुरक्षित सूचना प्रविधिको प्रयोगबाट पारदर्शी एवम् प्रभावकारी सार्वजनिक व्यवस्थापनको अपेक्षा गरिएको छ। सूचना प्रविधिको निरन्तर विकास, बढ्दो प्रयोग एवम् गतिशीलतासँगै सूचना प्रविधि प्रणालीमाथिको अनधिकृत पहुँचको समस्या दिनानुदिन बढ्दै गइरहेको छ। राज्य व्यवस्थाको सञ्चालन, विकासको व्यवस्थापन, सार्वजनिक सेवा प्रवाह तथा जनताका दैनिक क्रियाकलापहरू सूचना प्रविधिमा निर्भर हुँदै गइरहेको अवस्थामा सूचना प्रविधि प्रणालीलाई थप भरपर्दो र सुरक्षित बनाउन आवश्यक देखिएको छ। राष्ट्रिय तथा अन्तर्राष्ट्रियस्तरबाट सूचना प्रविधि प्रणालीमाथि भइरहेका साइबर आक्रमणको प्रतिरक्षा सुनिश्चित गर्नुपर्ने भएको छ। यस सन्दर्भमा सूचना प्रविधि प्रणालीमा साइबर आक्रमणबाट हुन सक्ने क्षतिलाई न्यूनिकरण र भविष्यमा हुन सक्ने यस्ता आक्रमणहरूबाट सुरक्षित रहन साइबर सुरक्षासम्बन्धी राष्ट्रिय नीति तर्जुमा गरिएको छ।

२. विगतको प्रयासः

नेपालमा पहिलो पटक वि.सं. २०२८ सालको राष्ट्रिय जनगणनाको तथ्याङ्क प्रशोधनका क्रममा कम्प्युटर प्रविधिको प्रयोग भएको हो। २०३१ सालमा कम्प्युटरसँग सम्बन्धित पहिलो संस्था सेन्टर फर इलेक्टोनिक डाटा प्रोसेसिङ्गको स्थापना भयो जसको नाम पछि परिवर्तन भएर राष्ट्रिय कम्प्युटर केन्द्र भएको हो। राष्ट्रिय सञ्चार नीति, २०४९, दूरसञ्चार ऐन, २०५३ र दूरसञ्चार नियमावली, २०५४ लागू भएपश्चात् मुलुकमा दूरसञ्चार क्षेत्र खुल्ला एवम् प्रतिस्पर्धी युगमा प्रवेश गरेको हो। वि.सं. २०५७ सालमा लागू भएको सूचना प्रविधि नीतिले सूचना प्रविधिलाई देश विकासको वृहत्तर लक्ष्य हासिल गर्ने औजारको रूपमा स्थापित गर्ने अवधारणा अघि सारेको थियो। त्यसैगरी, सूचना प्रविधिको उपयोगबाट सामाजिक एवम् आर्थिक विकासका लक्ष्यहरू हासिल गर्दै गरिबी न्यूनीकरण गर्ने लक्ष्यका साथ सूचना प्रविधि नीति, २०६७ जारी गरियो। उक्त नीतिमा सूचना प्रविधिको प्रयोगमा सूचनाको सुरक्षा एवम् तथ्याङ्कको गोपनीयतालाई सुदृढ गरिने विषयलाई जोड दिइएको थियो। सूचना तथा सञ्चार प्रविधि नीति, २०७२ मा सूचना प्रविधिको प्रयोगमा सुरक्षा एवम् विश्वासको प्रत्याभूति गरिने, साइबर अपराधको रोकथाम तथा अभियोजन प्रणालीको विकास गरिने, साइबर आक्रमण पहिचान, रोकथाम, प्रतिरक्षालगायतका आयामहरूलाई प्रभावकारी सम्बोधन गर्ने कुरामा जोड दिइएको छ। आवधिक योजनाहरूमा समेत साइबर सुरक्षाका विषयलाई जोड दिइएको छ।

विगतमा भएका प्रयासहरूबाट साइबर सुरक्षाका क्षेत्रमा केही कार्यहरू भएतापनि सूचना प्रविधिको बढ्दो प्रयोगसँगै साइबर सुरक्षामा नयाँ-नयाँ चुनौतीहरू देखापरेका छन्।

३. वर्तमान स्थितिः

नेपालको संविधानमा राष्ट्रिय आवश्यकता अनुसार सूचना प्रविधिको विकास र विस्तार गरी त्यसमा सर्वसाधारण जनताको सरल र सहज पहुँच सुनिश्चित गर्दै राष्ट्रिय विकासमा सूचना प्रविधिको उच्चतम उपयोग गर्ने विषयलाई राज्यका नीतिमा समावेश गरिएकोछ। विद्युतीय कारोवारलाई व्यवस्थित, सुरक्षित र भरपर्दो बनाउनुका साथै विद्युतीय अभिलेखमाथि अनधिकृत व्यक्तिको पहुँचलाई नियन्त्रण गर्ने उद्देश्यका साथ विद्युतीय कारोवार ऐन, २०६३ तथा विद्युतीय कारोवार नियमावली, २०६४ कार्यान्वयनमा रहेका छन्।

सूचना तथा सञ्चार प्रविधिको प्रयोगबाट सुशासन प्रवर्द्धन गर्ने लगायतका उद्देश्य राखी सूचना तथा सञ्चार प्रविधि नीति, २०७२ जारी भई कार्यान्वयनमा रहेको छ। यस नीतिले डिजिटल साक्षरतालाई जोड दिँदै सन् २०२० सम्ममा सम्पूर्ण नागरिकमा इन्टरनेट पहुँचको सुनिश्चित गर्ने तथा ८० प्रतिशत नागरिक लक्षित सेवाहरू अनलाइन मार्फत् प्रदान गर्ने लक्ष्य लिएकोछ। यस नीतिमा साइबर सुरक्षाको विषयलाई सम्बोधन गर्दै साइबर सुरक्षा निकायको स्थापना तथा साइबर आक्रमणको पहिचान, रोकथाम, प्रतिरक्षा लगायतका आयामहरूको प्रभावकारी रूपमा सम्बोधन गर्ने, साइबर सुरक्षा सम्बन्धी क्षमता अभिवृद्धि कार्यक्रम, आपतकालीन कम्प्युटर उद्धार समूह (Computer Emergency Response Team) को स्थापना गरी साइबर सुरक्षा सम्बन्धी चुनौतीहरू शीघ्र सम्बोधन गर्ने व्यवस्था मिलाइने उल्लेख गरिएकोछ।

सूचना प्रविधिको विकास तथा बढ्दो प्रयोगसँगै देखिएको साइबर सुरक्षा जोखिमको पहिचान, त्यसबाट हुने असरको न्यूनीकरण र आकस्मिक साइबर सुरक्षाको व्यवस्था गर्ने उद्देश्यले सूचना प्रविधि आकस्मिक सहायता समूह सञ्चालन तथा व्यवस्थापन निर्देशिका, २०७५ जारी भई कार्यान्वयनमा रहेको छ। उक्त निर्देशिकामा व्यवस्था भए अनुरूप राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह (National Information Technology Emergency Response Team) र राष्ट्रिय साइबर सुरक्षा अनुगमन केन्द्र स्थापना भई सरकारी सूचना प्रविधि प्रणालीहरूको निरन्तर अनुगमन भइरहेको छ।

चालू आवधिक योजनाले साइबर सुरक्षा तथा गोपनीयता सम्बन्धी कार्य गर्न साइबर सुरक्षा अनुगमन केन्द्र स्थापना गरी साइबर सुरक्षालाई प्रभावकारी बनाइने विषयलाई जोड दिएकोछ। डिजिटल नेपाल फ्रेमवर्क, २०७६ मा राष्ट्रिय साइबर सुरक्षा केन्द्रको स्थापना लगायतका साइबर सुरक्षासँग सम्बन्धित विषयहरूलाई समावेश गरिएको छ। नेपाल दूरसञ्चार प्राधिकरणद्वारा दूरसञ्चार तथा इन्टरनेट सेवा प्रदायकहरूको सूचना प्रविधि

प्रणालीलाई समेटिने गरी साइबर सुरक्षा विनियमावली, २०७७ (Cyber Security Byelaw, 2077) कार्यान्वयनमा ल्याइएकोछ। नेपाल सरकारको वार्षिक नीति तथा कार्यक्रममा साइबर सुरक्षा सम्बन्धी विषयलाई प्राथमिकताकासाथ उल्लेख गर्रिंदै आएको छ।

४. समस्या तथा चुनौतीः

सूचना तथा सञ्चार प्रविधिको तीव्र विकास र व्यापकतासँगै यसको सुरक्षा चुनौती विश्वको प्रमुख चासोको विषय बन्दै गएकोछ। सूचना तथा सञ्चार प्रविधि प्रणालीहरू माथिको साइबर आक्रमणको जोखिम दिनानुदिन बढ्दै गइरहेको छ। साइबर आक्रमण निश्चित भूगोलमा मात्र सीमित नभई विश्वव्यापीरूपमा भइरहेका छन्। साइबरसँग सम्बन्धित अपराधिक गतिविधिहरूमा वृद्धि हुँदै गएकाले व्यक्तिगत तथा संस्थागत विवरणहरूको गोपनीयता एवम् तथ्याङ्क लगायत सूचना प्रविधि प्रणालीको सुरक्षा गर्ने कार्य जटिल बन्दै गएकोछ। सूचना तथा सञ्चार प्रविधि प्रणालीमाथि राष्ट्रिय एवम् अन्तर्राष्ट्रियस्तरबाट हुने यस प्रकारका अनधिकृत पहुँच तथा आक्रमणका प्रयासलाई निस्तेज पार्न देहायका समस्या तथा चुनौती रहेका छन्:

४.१ समस्याः

४.१.१ साइबर सुरक्षाको लागि प्रभावकारी कानूनी व्यवस्था तथा संस्थागत संरचना नहुनु,

४.१.२ साइबर सुरक्षासम्बन्धी पूर्वाधारको कमी हुनु,

४.१.३ साइबर सुरक्षाको क्षेत्रमा दक्ष जनशक्तिको कमी हुनु,

४.१.४ साइबर सुरक्षासम्बन्धी सचेतनाको कमी हुनु।

४.१.५ साइबर सुरक्षा सम्बन्धमा आन्तरिक तथा वाह्य समन्वयमा कमी हुनु।

४.२ चुनौतीः

४.२.१ सूचना तथा सञ्चार प्रविधि प्रणालीमा हुने साइबर आक्रमणको जोखिम न्यून गर्नका लागि नीतिगत र संरचनागत व्यवस्था गर्नु,

४.२.२ साइबर सुरक्षाको सुनिश्चितता गर्न समयानुकुल दक्ष जनशक्ति विकास र उपयोग गर्नु,

४.२.३ राष्ट्रिय सम्वेदनशील पूर्वाधार (National Critical Infrastructure) को पहिचान एवम् संरक्षण गर्नु,

४.२.४ सार्वजनिक, व्यावसायिक र व्यक्तिगत सूचना तथा तथ्याङ्कमा अनधिकृत पहुँच नियन्त्रण गर्नु,

४.२.५ साइबर सुरक्षाका लागि राष्ट्रिय तथा अन्तर्राष्ट्रिय सहयोग प्राप्त गर्नु।

५. नीतिको आवश्यकताः

सूचना प्रविधिको क्षेत्रमा भएको तीव्र विकासले विश्वलाई एक गाउँ (Global Village) को रूपमा परिणत गरेकाले सूचना प्रविधिको उच्चतम प्रयोग गरी आर्थिक तथा सामाजिक रुपान्तरणका लक्ष्य प्राप्त गर्न विद्यमान नीतिगत तथा संस्थागत क्षमता पर्याप्त देखिँदैन। साइबर सुरक्षामा मुलुकलाई सबल र सक्षम बनाउनका लागि आवश्यक पर्ने नीतिगत र संरचनागत व्यवस्था गर्न आवश्यक देखिएको छ। हाम्रो सन्दर्भमा साइबर सुरक्षासम्बन्धी विषय नयाँ हुनुको साथै जटिल र चुनौतीपूर्ण समेत रहेको छ। यस क्षेत्रमा आवश्यक पर्ने दक्ष जनशक्तिको अभाव छ। साइबर सुरक्षा, बौद्धिक सम्पत्तिको संरक्षण, अन्तरक्षेत्रगत विषय सम्बोधन, सुरक्षा संवेदनशीलता र अभिसरण (Convergence) लगायतका विषयहरू सम्बोधन गर्नु पर्ने देखिएको छ। साइबर आक्रमण एवम् साइबर अपराध सीमाविहीन हुने भएकोले यसको नियन्त्रणका लागि अन्तर्राष्ट्रियस्तरमा सहयोग र सहकार्य गर्न आवश्यक देखिएको छ।

यस नीतिले सङ्कलित, प्रशोधित, सङ्ग्रहित, प्रकाशित एवम् प्रसारित सूचना, तथ्याङ्क एवं सूचना तथा सञ्चार प्रविधि प्रणालीको गोपनीयता, अखण्डता, उपलब्धता, प्रमाणिकता र आधिकारिकता (Confidentiality, Integrity, Availability, Authenticity and Authorization) को स्तरवृद्धि गर्न संवेदनशील पूर्वाधार प्रदायकहरूले सञ्चालन गरेका वा उपयोग गरेका सूचना प्रणालीको जोखिम व्यवस्थापन क्षमता वृद्धि गर्न समेत महत्त्वपूर्ण आधार निर्माण गर्ने हुँदा भरपर्दो, सुरक्षित एवम् उत्थानशील साइवरस्पेस निर्माणका लागि राष्ट्रिय साइबर सुरक्षा नीति तर्जुमा गर्न आवश्यक देखिएको छ।

६. दीर्घकालीन सोचः

भरपर्दो, सुरक्षित एवम् उत्थानशील साइबर स्पेश (Resilient Cyber Space) निर्माण।

७. परिदृश्यः

कानूनी र संस्थागत संरचना निर्माण, जनचेतना अभिवृद्धि र क्षमता विकास गर्दै विधि, प्रविधि र जनशक्तिको संयोजनबाट सूचना एवम् सूचना तथा सञ्चार प्रविधि प्रणालीलाई सुरक्षित बनाउने।

८. लक्ष्यः

विश्वव्यापी साइबर सुरक्षा सूचकाङ्क (Global Cyber Security Index-GCI) स्कोर (Score) ४४.९९ बाट आगामी पाँच वर्षभित्र ६०, दश वर्षभित्र ७० र पन्ध्र वर्षभित्र ८० प्रतिशत पुऱ्याउने।

९. उद्देश्यः

९.१ सुरक्षित साइबर स्पेस निर्माणका लागि कानूनी र संस्थागत व्यवस्था गर्नु,

९.२ साइबर आक्रमणको जोखिम न्यूनीकरण गर्दै संवेदनशील राष्ट्रिय पूर्वाधार संरक्षण गर्नु,

९.३ साइबर स्पेसलाई सशक्त र सुदृढ बनाउन साइबर सुरक्षा क्षेत्रमा जनशक्ति उत्पादन एवम् कार्यरत जनशक्तिको क्षमता अभिवृद्धि गर्नु,

९.४ साइबर सुरक्षासम्बन्धी जोखिम न्यूनिकरणका लागि द्विपक्षीय, क्षेत्रीय तथा अन्तर्राष्ट्रियस्तरमा समन्वय, अनुभव एवम् सहयोग आदान प्रदान गर्नु।

१०. रणनीतिः

१०.१ सुरक्षित, भरपर्दो र उत्थानशील साइबर स्पेस बनाउन आवश्यक कानून एवम् मापदण्डहरू तर्जुमा गर्ने,

१०.२ सूचना एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको सुरक्षा गर्न अन्तर्राष्ट्रिय प्रचलनसमेतको आधारमा संस्थागत संरचनाहरू निर्माण एवम् सुदृढीकरण गर्ने,

१०.३ साइबर सुरक्षालाई सुदृढ गर्न सबल एवम् सुरक्षित प्रविधि, पूर्वाधार र प्रक्रियाको व्यवस्था गरी संवेदनशील राष्ट्रिय पूर्वाधारको पहिचान गरी संरक्षण गर्ने,

१०.४ साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन र क्षमता विकास गर्ने,

१०.५ साइबर सुरक्षाको विषयमा जनचेतना अभिवृद्धि गर्ने,

१०.६ सुरक्षित साइबर स्पेस निर्माणका लागि सार्वजनिक निकाय तथा निजी क्षेत्रबीच समन्वय एवम् सहकार्य गर्ने,

१०.७ साइबर सुरक्षालाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय संघ- सँगनहरूसँग समन्वय एवम् सहकार्य गर्ने,

१०.८ सुरक्षित अनलाइन स्पेस निर्माण गर्ने,

१०.९ सफ्टवेयर विकासकर्ता एवम् आपूर्तिकर्तालाई जिम्मेवार बनाइने।

११. कार्यनीतिः

<u>रणनीति नं. १०.१ सँग सम्बन्धित</u> **(सुरक्षित, भरपर्दो र उत्थानशील साइबर स्पेस बनाउन आवश्यक कानून एवम् मापदण्डहरू तर्जुमा गर्ने ।)**

११.१ विद्यमान कानूनलाई साइबर सुरक्षा अनुकूल हुनेगरी संशोधन, परिमार्जन र पुनरावलोकन गरिनेछ।

११.२ सूचना तथा सञ्चार प्रविधिको दुरूपयोग गरी हुने साइबर अपराध (Cybercrime) विरुद्ध एवम् साइबर सुरक्षा सबलीकरणको लागि कानून तर्जुमा गरिनेछ।

११.३ साइबर अपराध अनुसन्धान, प्रमाण सङ्कलन, अभियोजन तथा नियन्त्रणका लागि अन्तर्राष्ट्रिय मापदण्डअनुरूप कानूनी तथा नीतिगत व्यवस्था गरिनेछ।

११.४ सूचनाको हक, गोपनीयताको हक लगायतका मौलिक अधिकारहरूको संरक्षणका सन्दर्भमा क्षेत्रीय एवम् अन्तर्राष्ट्रिय मापदण्डअनुरूप कानूनी तथा नीतिगत व्यवस्था गरिनेछ।

११.५ सूचना प्रविधिको माध्यमबाट सिर्जना हुने बौद्धिक सम्पत्ति तथा प्रतिलिपि अधिकार संरक्षणको लागि सम्बन्धित कानूनमा संशोधन र एकीकरण गरिनेछ।

११.६ साइबर आक्रमण तथा अपराधबाट सिर्जना हुने जोखिम बहन गर्न साइबर सुरक्षा बीमाको व्यवस्था गरिनेछ।

११.७ साइबर सुरक्षाका मापदण्डहरू कार्यान्वयनका लागि अन्तर्राष्ट्रिय मापदण्डसमेतका आधारमा राष्ट्रिय साइबर सुरक्षा फ्रेमवर्क तर्जुमा गरिनेछ।

११.८ संवेदनशील पूर्वाधार जोखिम आकलन तथा न्यूनीकरण (Risk assessment and Mitigation) एवम् घटना प्रतिक्रिया योजनाहरू (Incident Response Plans) को निर्माण गरी कार्यान्वयन गरिनेछ।

११.९ साइबर सुरक्षा प्रक्रियामा तयारी, संरक्षण, पहिचान, प्रतिक्रिया तथा पुनर्लाभ (Preparedness, Protection, Detection, Response and Recovery) सम्बन्धी कार्य योजना तयार गरी कार्यान्वयन गरिनेछ।

११.१० राष्ट्रिय साइबर सुरक्षा रणनीतिको लागि प्राविधिक मार्गदर्शन (Technical Guidelines) को विकास गरिनेछ।

११.११ गुणस्तरीय सफ्टवेयर, हार्डवेयर, नेटवर्क डिभाइसको निर्माण, आयात तथा प्रयोग सम्बन्धी मापदण्ड तयार गरी लागू गरिनेछ।

११.१२ साइबर सुरक्षासम्बन्धी अन्तर्राष्ट्रिय अभ्याससमेतका आधारमा न्यूनतम प्राविधिक मापदण्ड (Minimum Technical Standard) निर्माण गरिनेछ।

११.१३ साइबर सुरक्षा परीक्षणको मापदण्ड र परीक्षक (Auditor) को योग्यता निर्धारण गरिनेछ।

११.१४ विभिन्न उत्पादन वा सेवाहरू बीच अन्तरसञ्चालन र डाटा आदानप्रदानलाई सहज बनाउन खुला मापदण्डहरूको प्रयोगलाई प्रोत्साहन गरिनेछ।

<u>रणनीति नं. १०.२ सँग सम्बन्धित</u> (सूचना एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको सुरक्षा गर्न अन्तर्राष्ट्रिय प्रचलनसमेतको आधारमा संस्थागत संरचनाहरू निर्माण एवम् सुदृढीकरण गर्ने।)

११.१५ साइबर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्धन, जनचेतना अभिवृद्धि, साइबर सुरक्षासम्बन्धी तयारी, रोकथाम, पहिचान, प्रतिक्रिया तथा पुनर्लाभ गर्न सातै दिन चौविसै घण्टा (२४/७) सम्पर्क निकायको रूपमा कार्य गर्न, डिजिटल फोरेन्सिक अनुसन्धान गर्न तथा साइबर सुरक्षासँग सम्बन्धित निकायको नियमनकारी निकायको रूपमा समेत कार्य गर्ने गरी राष्ट्रिय साईबर सुरक्षा केन्द्र स्थापना गरिनेछ।

११.१६ सूचना प्रविधि क्षेत्रको प्रवर्द्धन, नियमन तथा सरकारी निकायहरूका लागि आवश्यक पर्ने सूचना प्रविधि प्रणालीको विकास एवम् नियमन गर्ने गरी सूचना प्रविधि विभागको क्षेत्राधिकार विस्तार गरिनेछ।

११.१७ साइबर सुरक्षा र साइबर अपराध अनुसन्धानसम्बन्धी विद्यमान संस्थाहरूको क्षमता अभिवृद्धि गरिनेछ।

११.१८ साईबर सुरक्षासम्बन्धी आक्रमणहरूका बारेमा सूचना आदानप्रदान गर्न डिजिटल पूर्वाधार (Digital Infrastructure) को विकास गरिनेछ।

११.१९ साइबर सुरक्षासम्बन्धी राष्ट्रिय आकस्मिक योजना (National Contingency Plan) तयार गरी कार्यान्वयन गरिनेछ।

११.२० साइबर सुरक्षासम्बन्धी क्रियाकलापको समन्वय एवम् प्राथमिकीकरणका लागि राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह गठन गरी क्रियाशील बनाईनेछ।

११.२१ नेपाल सूचना प्रविधि आकस्मिक सहायता समूह तथा क्षेत्रगत सूचना प्रविधि आकस्मिक सहायता समूह र प्रदेशमा प्रादेशिक सूचना प्रविधि आकस्मिक सहायता समूहको गठन गरी क्रियाशील तुल्याइनेछ। साथै संघ, प्रदेश र स्थानीय तहको समन्वय र सहकार्यमा साइबर सुरक्षा सूचना सञ्जाल विकास गरिनेछ।

११.२२ व्यवसायिक योजनाहरूमा एकीकृत सूचना सुरक्षा नीतिहरू समावेश गर्न संस्थाहरूलाई प्रोत्साहित गरिनेछ।

११.२३ राष्ट्रियस्तरमा सार्वजनिक निजी साझेदारीको निरीक्षण गर्न राष्ट्रिय साइबर सुरक्षा केन्द्रलाई सशक्त बनाईनेछ।

<u>रणनीति नं. १०.३ सँग सम्बन्धित</u> ***(साइबर सुरक्षालाई सुदृढ गर्न सबल एवम् सुरक्षित प्रविधि, पूर्वाधार र प्रक्रियाको व्यवस्था गरी संवेदनशील राष्ट्रिय पूर्वाधारको संरक्षण गर्ने।)***

११.२४ सूचना तथा सञ्चार प्रविधि प्रयोग हुने राष्ट्रिय संवेदनशील पूर्वाधारहरू (National Critical Infrastructures)को पहिचान एवम् संरक्षण गर्ने व्यवस्था मिलाइनेछ।

११.२५ संवेदनशील तथ्याङ्क सङ्कलन, प्रशोधन, प्रयोग तथा भण्डारण गर्ने सार्वजनिक निकाय तथा निजी क्षेत्रका संस्थालाई आवधिकरूपमा साइबर सुरक्षा परीक्षण अनिवार्य गरिनेछ।

११.२६ नागरिकहरूको अनलाईन पहिचानको सुरक्षा तथा डाटा सुरक्षासम्बन्धी व्यवस्था गरिनेछ।

११.२७ व्यक्तिगत वा संस्थागत तथ्याङ्कहरू सङ्कलन, प्रशोधन, प्रयोग एवम् भण्डारण गर्ने निकायहरूमा भएका साइबर आक्रमण तथा प्रयोगकर्ताका डाटा हानी, नोक्सानी, तथा चोरीसम्बन्धी सूचना सार्वजनिक गर्न अनिवार्य गरिनेछ।

११.२८ साइबर सुरक्षासम्बन्धी पूर्वाधारको निर्माण तथा स्तरोन्नती गरिनेछ।

११.२९ साइबर सुरक्षासम्बन्धी परीक्षण एवम् प्रमाणीकरणका लागि प्रचलित कानून, मापदण्ड, निर्देशिका एवम् असल अभ्यास (जस्तैः ISO 27001) अनुरुप गर्ने व्यवस्था मिलाइनेछ।

११.३० साइबर सुरक्षा विकासका सूचकहरूको निर्माण गरी राष्ट्रिय साइबर सुरक्षा परिपक्वता (National Cyber Security Maturity) मापन गरिनेछ।

११.३१ विद्युतीय माध्यमबाट प्रवाह हुने सेवालाई सुरक्षित र भरपर्दो बनाइनेछ।

११.३२ सरकारी निकायहरूको एप्लिकेशन सफ्टवेयर र ईमेलमा विद्युतीय हस्ताक्षरको प्रयोग अनिवार्य गर्ने व्यवस्था मिलाइनेछ।

११.३३ विद्युतीय माध्यमबाट प्रवाह हुने डाटा सुरक्षित र भरपर्दो बनाइनेछ।

११.३४ सार्वजनिक तथा सेवाप्रदायक निकायले प्रयोग गर्ने हार्डवेयर, सफ्टवेयर र नेटवर्कहरूको नियमित सुरक्षण परीक्षण गर्ने व्यवस्था मिलाइनेछ।

११.३५ विश्वसनीय र स्वदेशी सूचना तथा सञ्चार प्रविधि सम्बन्धी उत्पादनहरू खरिद तथा प्रयोगलाई प्रोत्साहित गरिनेछ।

११.३६ सूचना प्रविधि प्रणालीको सुदृढीकरण गर्न इथिकल ह्याकिङ (Ethical Hacking)लाई प्रोत्साहन गरिनेछ।

१०.१० <u>रणनीति नं. १०.४ सँग सम्बन्धित</u> ***(साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन र क्षमता विकास गर्ने।)***

११.३७ साइबर सुरक्षासम्बन्धी विषयलाई विद्यालयस्तरको पाठ्यक्रममा समावेश गरिनेछ।

११.३८ साइबर सुरक्षा सम्बन्धी दक्ष जनशक्ति उत्पादन गर्न साइबर सुरक्षाको क्षेत्रमा कार्य गर्ने संघ-संस्थासँगको सहकार्यमा साइबर सुरक्षा फिनिसिङ्ग स्कूल (Finishing School) को व्यवस्था गरिनेछ।

११.३९ राष्ट्रिय तथा अन्तर्राष्ट्रिय विश्वविद्यालयहरूसँगको सहकार्यमा साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन गरिनेछ।

११.४० साइबर सुरक्षासम्बन्धी अध्ययन, अनुसन्धान तथा विकासका लागि विश्वविद्यालयहरूलाई प्रोत्साहित गरिनेछ।

११.४१ साइबर सुरक्षा क्षेत्रमा कार्यरत सार्वजनिक निकायका जनशक्तिको क्षमता अभिवृद्धिका लागि अन्तर्राष्ट्रिय मापदण्डअनुरूपका तालिमको व्यवस्था गरिनेछ।

११.४२ नेपाल सूचना प्रविधि आकस्मिक सहायता समूहको क्षमता अभिवृद्धि गरिनेछ।

११.४३ साइवर सुरक्षालाई विशिष्टीकृत सेवाको रूपमा स्थापित गर्न सार्वजनिक सेवामा छुट्टै साइवर सुरक्षा समूह स्थापना गरिनेछ।

११.४४ सरकारी निकायहरूमा आवश्यकता अनुसार साइबर सुरक्षासँग सम्बन्धित दक्ष जनशक्ति व्यवस्था गरिनेछ।

११.४५ सार्वजनिक तथा निजी क्षेत्रका सूचना सुरक्षा पेशाकर्मीहरू (Information Security professionals) को योग्यता पहिचान गरी नियमित क्षमता विकास गर्ने व्यवस्था गरिनेछ।

११.४६ संवेदनशील सेवा प्रदायकहरू समेटिनेगरी वार्षिकरूपमा राष्ट्रिय साइबर ड्रिल आयोजना गरिनेछ।

<u>रणनीति नं. १०.५ सँग सम्बन्धित</u> *(साइबर सुरक्षाको विषयमा जनचेतना अभिवृद्धि गर्ने।)*

११.४७ समुदायमा साइबर सुरक्षासम्बन्धी जनचेतना अभिवृद्धिका लागि सामुदायिक साइबर सुरक्षा समूह गठन गरी परिचालन गरिनेछ।

११.४८ साइबर सुरक्षाको जोखिमबाट सुरक्षित रहन समुदायस्तरसम्म जनचेतना अभिवृद्धि कार्यक्रमहरू सञ्चालन गरिनेछ।

११.४९ ज्येष्ठ नागरिक, महिला तथा बालबालिका, विशेष आवश्यकता भएका व्यक्तिहरू तथा नागरिक समाजलाई लक्षित गरी साइबर सुरक्षासम्बन्धी जनचेतना कार्यक्रमहरू सञ्चालन गरिनेछ।

११.५० साइबर सुरक्षासम्बन्धी सार्वजनिक चासोका विषय, घटना, आदिको बारेमा नागरिकलाई सुसुचित गर्न आवश्यकता अनुसार निर्देशन (Advisory) जारी गरिनेछ।

११.५१ साइबर सुरक्षासम्बन्धी जनचेतनामूलक सामग्रीहरू निर्माण, वितरण र प्रसारण गरिनेछ।

रणनीति नं. १०.६ सँग सम्बन्धित ***(सुरक्षित साइबर स्पेस निर्माणका लागि सार्वजनिक निकाय तथा निजी क्षेत्रबीच समन्वय एवम् सहकार्य गर्ने।)***

११.५२ सार्वजनिक निजी साझेदारी [Public–private partnership- (PPP)] को अवधारणाअनुरूप साइबर सुरक्षा पूर्वाधारहरूको विकास गरिनेछ।

११.५३ साइबर जोखिमलाई न्यूनीकरण गर्न निजी क्षेत्रसँग सहकार्य गरिनेछ।

११.५४ साइबर सुरक्षासम्बन्धी कार्य गर्ने संघसंस्थाहरूलाई प्रोत्साहन गरिनेछ।

११.५५ साइबर सुरक्षाको क्षेत्रमा कार्यरत संघसंस्थाहरूको नियमनको व्यवस्था मिलाइनेछ।

रणनीति नं. १०.७ सँग सम्बन्धित ***(साइबर सुरक्षालाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय संघ-सँगठनहरूसँग समन्वय एवम् सहकार्य गर्ने।)***

११.५६ साईबर सुरक्षासम्बन्धी विषयमा अन्तर्राष्ट्रिय सहकार्यका लागि एउटै सम्पर्क विन्दु (Focal Point) तोकिनेछ।

११.५७ साइबर सुरक्षा अभिवृद्धि, क्षमता अभिवृद्धि, सूचना आदान-प्रदान र पारस्परिक कानुनी सहयोगमा सहजीकरण एवम् साइबर अपराध नियन्त्रण गर्न द्विपक्षीय एवम् बहुपक्षीय समझदारी गरिनेछ।

११.५८ साइबर सुरक्षा व्यवस्थालाई समयानुकूल परिष्कृत एवम् परिमार्जन गर्न अन्तर्राष्ट्रिय क्षेत्रमा अवलम्बन गरिएका असल अभ्यास एवम् नविनतम अवधारणा र प्रविधिको अवलम्बन गरिनेछ।

११.५९ साइबर सुरक्षासम्बन्धी अन्तर्राष्ट्रिय एवम् क्षेत्रीय सम्झौताहरूको कार्यान्वयन एवम् बाध्यात्मक मापदण्डहरू लागू गरिनेछ।

११.६० साइबर सुरक्षासम्बन्धी विश्वव्यापी जोखिमलाई न्यूनीकरण गर्न साइबर सुरक्षा क्षेत्रमा कार्यरत क्षेत्रीय एवम् अन्तर्राष्ट्रिय संगठनहरूसँग आबद्ध भई सहकार्य गरिनेछ।

रणनीति नं. १०.८ सँग सम्बन्धित ***(सुरक्षित अनलाइन स्पेस निर्माण गर्ने।)***

११.६१ इन्टरनेट तथा सामाजिक सञ्जालको प्रयोग गरी भ्रामक जानकारी सम्प्रेषण गर्ने कार्यलाई नियन्त्रण गरिनेछ।

११.६२ बालबालिकाका लागि अनुपयुक्त अनलाइन सेवाहरूमा पहुँच निषेध गरिनेछ।

११.६३ इन्टरनेट तथा सामाजिक सञ्जालको प्रयोगमार्फत हुने लैंगिक हिंसा, जातिवाद र भेदभाव लाई नियन्त्रण गरिनेछ।

११.६४ राष्ट्रिय सुरक्षामा आँच पुऱ्याउने, घृणा वा द्वेष फैलाउने, अनलाइन उत्पीडन (Online harassment) र साइबर बुलिङ्ग गर्ने, सामाजिक सद्भावमा खलल पुऱ्याउने किसिमका डिजिटल सामग्रीको सम्प्रेषणलाई नियन्त्रण गरिनेछ।

११.६५ स्प्याम (Spam) मेसेजहरू सम्प्रेषण गर्ने कार्यलाई नियमन गरिनेछ।

<u>रणनीति नं. १०.९ सँग सम्बन्धित</u> *(सफ्टवयर विकासकर्ता एवम् आपूर्तिकर्तालाई जिम्मेवार बनाइने।)*

११.६६ सफ्टवेयर विकासकर्तालाई आफूले विकास गरेको सफ्टवेयरको गुणस्तर एवम् सुरक्षाको सुनिश्चितताका लागि जिम्मेवार बनाइनेछ।

११.६७ सफ्टवेयर आपूर्तिकर्तालाई आफूले आपूर्ति गरेको सफ्टवेयरको गुणस्तर एवम् सुरक्षाको सुनिश्चितताका लागि जिम्मेवार बनाइनेछ।

१२. संस्थागत व्यवस्थाः

१२.१ <u>विषयगत निकायहरूको भूमिका र जिम्मेवारी</u>

यस नीतिको कार्यान्वयनमा नेतृत्वदायी भूमिका सञ्चार तथा सूचना प्रविधि मन्त्रालयको हुनेछ। क्षेत्रगत रणनीति एवम् कार्यनीतिहरूको प्रभावकारी कार्यान्वयन गर्ने जिम्मेवारी विषयगत मन्त्रालयहरूको हुनेछ।

१२.२ <u>निर्देशक समिति</u>

यस नीतिको समग्र निर्देशन, सहजीकरण तथा मार्गदर्शनको लागि देहाय बमोजिमको निर्देशक समिति गठन गरिनेछः

(क) मन्त्री सञ्चार तथा सूचना प्रविधि मन्त्रालय	अध्यक्ष
(ख) गभर्नर, नेपाल राष्ट्र बैङ्क	सदस्य
(ग) सचिव, प्रधानमन्त्री तथा मन्त्रिपरिषदको कार्यालय	सदस्य
(घ) सचिव, गृह मन्त्रालय	सदस्य
(ङ) सचिव, अर्थ मन्त्रालय	सदस्य
(च) सचिव, रक्षा मन्त्रालय	सदस्य
(छ) सचिव,संघीय मामिला तथा सामान्य प्रशासन मन्त्रालय	सदस्य
(ज) सचिव, शिक्षा विज्ञान तथा प्रविधि मन्त्रालय	सदस्य
(झ) सचिव, सञ्चार तथा सूचना प्रविधि मन्त्रालय	सदस्य सचिव

१२.३ **<u>समन्वय तथा सहजीकरण समितिः</u>**

यस नीतिको कार्यान्वयनको लागि अन्तरनिकाय समन्वय एवम् सहजीकरण गर्न देहाय बमोजिमको समन्वय तथा सहजीकरण समिति रहनेछः

(क) सचिव, सञ्चार तथा सूचना प्रविधि मन्त्रालय	अध्यक्ष
(ख) सहसचिव, प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय	सदस्य
(ग) सहसचिव, शिक्षा, विज्ञान तथा प्रविधि मन्त्रालय	सदस्य
(घ) सहसचिव, गृह मन्त्रालय	सदस्य
(ङ) सहसचिव, अर्थ मन्त्रालय	सदस्य
(च) सहसचिव, रक्षा मन्त्रालय	सदस्य
(छ) सहसचिव, परराष्ट्र मन्त्रालय	सदस्य
(ज) सहसचिव, महिला बालबालिका तथा समाज कल्याण मन्त्रालय	सदस्य
(झ) डेपुटी गभर्नर, नेपाल राष्ट्र बैङ्क	सदस्य
(ञ) अध्यक्ष, नेपाल दूरसञ्चार प्राधिकरण	सदस्य
(ट) मन्त्रालयले मनोनयन गरेका निजी क्षेत्र तथा नागरिक समाजका विषय विज्ञ प्रतिनिधि (कम्तिमा १जना महिला सहित २ जना)	सदस्य
(ठ) विश्वविद्यालयका प्राज्ञिकमध्येबाट मन्त्रालयले मनोनयन गरेको विषय विज्ञ (१ जना)	सदस्य
(ड) सहसचिव, सूचना प्रविधि महाशाखा सञ्चार तथा सूचना प्रविधि मन्त्रालय	सदस्य- सचिव

समन्वय समितिको काम, कर्तव्य र अधिकार

(क) यस नीतिको प्रभावकारी कार्यान्वयनको लागि आवश्यक कार्ययोजना तयार गरी निर्देशक समितिसमक्ष पेश गर्ने।

(ख) यस नीतिअन्तर्गत सञ्चालन हुने कार्यक्रम तथा क्रियाकलापहरूको प्रभावकारी कार्यान्वयनमा समन्वय, सहजीकरण, अनुगमन तथा मुल्याङ्कन गर्ने।

(ग) राष्ट्रिय संवेदनशील सूचना पूर्वाधार संरक्षणको निरीक्षण गर्ने।

(घ) निर्देशक समितिद्वारा निर्देशन भएका अन्य कार्यहरू गर्ने।

१२.४ **राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह (National Cyber Security Strategy Working Group – NCSWG) :**

(क) कार्यसमूहको संरचनाः

साइबर सुरक्षालाई मजवुत बनाउन देहायका सदस्यहरू रहनेगरी राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह गठन गरिनेछ।

१)	सहसचिव, सूचना प्रविधि महाशाखा, सञ्चार तथा सूचना प्रविधि मन्त्रालय	संयोजक
२)	महानिर्देशक, सूचना प्रविधि विभाग	सदस्य
३)	नियन्त्रक, प्रमाणिकरण नियन्त्रकको कार्यालय	सदस्य
४)	कार्यकारी निर्देशक, राष्ट्रिय सूचना प्रविधि केन्द्र	सदस्य
५)	निर्देशक, नेपाल दूरसञ्चार प्राधिकरण	सदस्य
६)	निर्देशक,नेपाल राष्ट्र बैङ्क	सदस्य
७)	उपसचिव (सूचना प्रविधि), प्रधानमन्त्री तथा मन्त्रिपरिषदको कार्यालय	सदस्य
८)	उपसचिव (सूचना प्रविधि), रक्षा मन्त्रालय	सदस्य
९)	उपसचिव (सूचना प्रविधि), गृह मन्त्रालय	सदस्य
१०)	नेपाली सेना, रा.प. द्वि. श्रेणी वा सो सरहको अधिकृत	सदस्य
११)	नेपाल प्रहरी, रा.प. द्वि. श्रेणी वा सो सरहको को अधिकृत	सदस्य
१२)	सशस्त्र प्रहरीबल, रा.प. द्वि. श्रेणी वा सो सरहको अधिकृत	सदस्य
१३)	राष्ट्रिय अनुसन्धान विभाग, रा.प. द्वि. श्रेणी वा सो सरहको अधिकृत	सदस्य
१४)	विश्वविद्यालयका प्राज्ञिक मध्येबाट मन्त्रालयले मनोनयन गरेको (१जना)	सदस्य
१५)	मन्त्रालयले मनोनयन गरेको निजी क्षेत्रको विज्ञ प्रतिनिधि (१जना)	सदस्य
१६)	उपसचिव, साइबर सुरक्षा शाखा सञ्चार तथा सूचना प्रविधि मन्त्रालय	सदस्य सचिव

(ख) <u>कार्य समूहको काम र कर्तव्यः</u>

यस कार्यसमूहले देहायका कार्यहरू गरी राष्ट्रिय समन्वय एवम् सहजीकरण समितिमा पेश गर्नेछ।

१) साइबर सुरक्षासम्बन्धी ऐन, नियम, नीति, रणनीति, मापदण्ड र कार्ययोजनामा समसामयिक सुधारका क्षेत्र पहिचान गर्ने।

२) साइबर सुरक्षासम्बन्धी क्रियाकलापको समन्वय एवम् प्राथमिकीकरण गर्ने।

३) सूचना सुरक्षा पेशाकर्मीहरू (Information Security professionals) का लागि आवश्यक न्यूनतम योग्यताको पहिचान गर्ने।

४) स्थानीय साइबर सुरक्षा समुदायको निर्माण र सशक्तीकरणमा सहजीकरण गर्ने।

५) साइबर सुरक्षाका घटनाहरूको विश्लेषण गर्ने।

६) साइबर आक्रमणको सम्भावित जोखिमलाई ध्यानमा राखी चाल्नुपर्ने कदमहरू निर्धारण गर्ने।

७) जोखिम आकलन एवम् आपतकालीन योजनाहरू तथा सम्भाव्य जोखिम न्यूनीकरणका उपायहरू पहिचान गर्ने।

१२.५ <u>नेपाल सूचना प्रविधि आकस्मिक सहायता समूह (NITERT) :</u>

सरकार, सरकारी संस्थाहरू, निजी क्षेत्र एवम् जनतालाई साइबर सुरक्षासँग सम्बन्धित सेवा प्रदान गर्ने जिम्मेवारीसहित विभिन्न क्षेत्रका विज्ञ प्रतिनिधि रहनेगरी नेपाल सूचना प्रविधि आकस्मिक सहायता समूहको गठन गरिनेछ। समूहले राष्ट्रिय स्तरमा साइबर सुरक्षा सम्बन्धी सचेतनाका कार्यक्रमहरु सञ्चालन गर्ने, साइबर अभ्यास (Cyber Drill) हरू सञ्चालन गर्ने, सर्वसाधारणसँग सूचना आदान-प्रदान गर्ने, अनलाइन बाल संरक्षणका मुद्दाहरूमा योगदान पुर्‍याउने, क्षेत्रीय र अन्तर्राष्ट्रिय संस्थाहरूसँग सम्बद्धता र सहयोग लगायतका कार्यहरू गर्नेछ।

१२.६ <u>**महिला तथा बालबालिका अनलाइन सुरक्षा कार्यसमूह (Women and Child Online Protection Working Group – WCOPWG):**</u>

(क) महिला तथा बालबालिकाको अनलाइन सुरक्षासम्बन्धी कार्यका लागि एक कार्यसमूह गठन हुनेछ। कार्यसमूहको गठन महिला तथा बालबालिकाको विषय हेर्ने मन्त्रालयले गर्नेछ।

(ख) कार्यसमूहले महिला तथा बाल अनलाइन सुरक्षाका सम्बन्धमा ध्यान दिनुपर्ने आवश्यक क्षेत्रहरू (जस्तैः प्राविधिक सुरक्षाका उपायहरू, विद्यालयका लागि

पाठ्यक्रम र आमाबुबा तथा अभिभावकहरूका लागि सूचना सामग्री) को पहिचान गर्नेछ।

(ग) कार्यसमूहले महिला तथा बालबालिकाको अनलाइन सुरक्षा गर्न सेवा प्रदायकहरूले अपनाउनुपर्ने विभिन्न प्राविधिक उपायहरूको निर्धारण गर्नेछ।

(घ) कार्यसमूहले सरोकारवाला निकायसँगको सहकार्यमा महिला तथा बालबालिकाको अनलाइन सुरक्षासम्बन्धी निर्देशिका तयार गरी कार्यान्वयन गर्नेछ।

१३. आर्थिक पक्षः

साइबर सुरक्षा नीतिको लक्ष्य प्राप्तिको लागि राष्ट्रिय एवम् अन्तर्राष्ट्रिय स्रोत तथा साधनको परिचालन गरिनेछ।

१४. कानूनी व्यवस्थाः

नीति कार्यान्वयनका लागि आवश्यक कानूनहरूको निर्माण एवम् विद्यमान कानूनहरूको पुनरावलोकन गरिनेछ।

१५. अनुगमन र मूल्याङ्कनः

१) नीति कार्यान्वयनको अनुगमन गर्न मुख्य जिम्मेवारी राष्ट्रिय समन्वय तथा सहजीकरण समितिको हुनेछ।

२) यस नीतिको वार्षिकरूपमा समीक्षा गरी आवधिक रूपमा पुनरावलोकन गरिनेछ।

१६. जोखिमः

(क)सरोकारवालाको सहयोग प्राप्त गर्न कठिनाइ हुन सक्ने।

(ख)संवेदनशील पूर्वाधार प्रदायकहरूले प्रदान गर्ने सेवाहरूको सुरक्षा र सूचना प्रणालीमा पहुँच गर्न कठिनाइ हुन सक्ने।

(ग) साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति व्यवस्थापनमा कठिनाइ हुनसक्ने।