सेन्टर फर मिडिया रिसर्च – नेपाल

नीति पत्र

नीति पत्र शृङ्खला नं. ४१

भाद्र, २०८०

राष्ट्रिय साइबर सुरक्षा नीति २०८० को विश्लेषण

भक्तिराम घिमिरे (अधिवक्ता)

पृष्ठभूमि

अबको नेपालको समृद्धि र सुरक्षा आगामी दिनमा हामीले कसरी साइबर स्पेस र यसका चुनौतीलाई सामना गर्छौं भन्नेमा निर्भर गर्छ । सूचना प्रविधिमा भएको तीव्र विकासले अनगिन्ती अवसर ल्याएको छ तथापि अवसरसँगै बढ्दै गएको चुनौती तथा जोखिम पनि नकार्न सकिँदैन । राज्य व्यवस्थाको सञ्चालन, विकासको व्यवस्थापन, सार्वजनिक सेवा प्रवाह तथा नागरिकका दैनिक क्रियाकलाप डिजिटल प्रविधिमा निर्भर हुँदै गइरहेको अवस्थामा साइबर सुरक्षा चुनौतीपूर्ण हुँदै गएको छ । दिनानुदिन बढ्दै गइरहेको व्यक्तिगत, संस्थागत डाटा चोरी/दुरूपयोग, सूचना प्रविधि प्रणालीहरूमाथिको अनधिकृत पहुँच, राष्ट्रिय तथा अन्तर्राष्ट्रिय सूचना प्रविधि प्रणालीमाथि भइरहेका साइबर आक्रमणको प्रतिरक्षा गर्ने विषयलाई सुनिश्चित गर्न साइबर आक्रमणबाट हुन सक्ने क्षति रोक्न, न्यूनीकरण गर्न र भविष्यमा हुन सक्ने यस्ता आक्रमणबाट सुरक्षित रहनु अत्यावश्यक भएको छ ।

एकातर्फ सुरक्षित सूचना प्रविधिको प्रयोगबाट पारदर्शी एवम् प्रभावकारी सार्वजनिक सेवा व्यवस्थापनको अपेक्षा पूरा गर्नुपर्ने अवस्था छ भने अर्कोतर्फ नागरिक अधिकारका विश्वव्यापी मान्यता, नेपालको संविधानले प्रदत्त गरेको मौलिक हक कार्यान्वयन गर्नुपर्ने अवस्थासमेत छ । यसका साथै राष्ट्रिय तथा अन्तर्राष्ट्रिय स्तरमा सूचना प्रविधि प्रणालीमा भइरहेको साइबर आक्रमणको प्रतिरक्षा सुनिश्चित गर्नुपर्ने पक्षमा समेत ध्यान जानु उत्तिकै आवश्यक छ । हामी साइबर स्पेसको प्रयोगबाट टाढा रहन सक्दैनौं । यसको दायरा सङ्कुचन गरेर होइन, सुरक्षित गरेर प्रयोग गरेको खण्डमा यो चुनौती मात्र नभई अवसरका रूपमा बदलिन सक्छ ।

नेपालको सूचना प्रविधिसम्बन्धी विगत र वर्तमान स्थिति

नेपालमा पहिलो पटक २०२८ सालमा राष्ट्रिय

जनगणनाको तथ्याङ्क प्रशोधनका क्रममा कम्प्युटर प्रविधिको प्रयोग भएको हो । २०३१ सालमा कम्प्युटरसँग सम्बन्धित पहिलो संस्था सेन्टर फर इलेक्ट्रोनिक डाटा प्रोसेसिङ स्थापना भयो जसको नाम पछि राष्ट्रिय कम्प्युटर केन्द्र भएको हो ।[१]

राष्ट्रिय सञ्चार नीति २०४९, दूरसञ्चार ऐन, २०५३ र दूरसञ्चार नियमावली, २०५४ लागु भएपश्चात मुलुकमा दूरसञ्चार क्षेत्र खुला एवम् प्रतिस्पर्धी युगमा प्रवेश गरेको हो । २०५७ सालमा लागु भएको सूचना प्रविधि नीतिले सूचना प्रविधिलाई देश विकासको बृहत्तर लक्ष्य हासिल गर्ने औजारका रूपमा स्थापित गर्ने अवधारणा अघि सारेको थियो । त्यसैगरी सूचना प्रविधिको उपयोगबाट सामाजिक एवम् आर्थिक विकासका लक्ष्यहरु हासिल गर्दै गरिबी न्यूनीकरण गर्ने लक्ष्यका साथ सूचना प्रविधि नीति, २०६७ जारी गरियो । उक्त नीतिमा प्रविधि प्रयोगमा सूचनाको सुरक्षा एवम् तथ्याङ्कको गोपनीयतालाई सुदृढ गरिने विषयमा जोड दिइएको थियो ।

नवौं योजना (२०५४-२०५९) मा विद्यालयहरूमा कम्प्युटर शिक्षा व्यापकरूपमा विस्तार गर्ने, उच्च अध्ययनका लागि औपचारिक शिक्षा तथा उच्च तालिम व्यवस्था गर्ने, स्तरीय विद्यालय र सूचना प्रविधि पार्क स्थापना गर्ने र सरकारी कार्यालयमा योजना तर्जुमा र व्यवस्थापनमा कम्प्युटर उपयोगमा जोड दिनेलगायतका नीति कार्यक्रम थियो । तर योजना अवधिमा सूचना प्रविधि शिक्षाको विकास र विस्तारका लागि ४ वटा विश्वविद्यालयलाई अनुदान सहयोग उपलब्ध गराइएको, सूचना प्रविधि नीति, २०५७ जारी गरिएको र विद्युतीय कारोबार ऐन, नियम तयार गरिएको तथा बनेपामा सूचना प्रविधि पार्कको निर्माण सुरू गरिएको पाइन्छ ।

राष्ट्रिय आवश्यकताअनुसार सूचना प्रविधिको विकास र विस्तार गरी त्यसमा सर्वसाधारण जनताको सहज र सरल पहुँच सुनिश्चित गर्ने तथा राष्ट्रिय विकासमा सूचना प्रविधिको उच्चतम उपयोग गर्ने[२] राज्यको नीति छ । विद्युतीय तथ्याङ्क आदान-प्रदानको माध्यमबाट वा अन्य कुनै विद्युतीय सञ्चार माध्यमबाट हुने कारोबारलाई भरपर्दो र सुरक्षित बनाइ विद्युतीय अभिलेख सिर्जना, उत्पादन, प्रशोधन, सञ्चय, प्रवाह तथा सम्प्रेषण प्रणालीको मान्यता, सत्यता, अखण्डता र विश्वसनीयतालाई प्रमाणीकरण तथा नियमित गर्ने व्यवस्था गर्न र विद्युतीय अभिलेखलाई अनधिकृततवरबाट प्रयोग गर्न वा त्यस्तो अभिलेखमा गैरकानुनीतवरबाट परिवर्तन गर्ने कार्यलाई नियन्त्रण गर्नका लागि[३] पहिलो कानुनीरूपमा विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ तथा विद्युतीय कारोबार नियमावली, २०६४ कार्यान्वयनमा छन् ।

सूचना तथा सञ्चार प्रविधिको प्रयोगबाट सुशासन प्रबर्द्धन गर्नेलगायतका उद्देश्य राखी सूचना तथा सञ्चार प्रविधि नीति, २०७२ जारी भई कार्यान्वयनमा छ । यस नीतिमा साइबर सुरक्षाको विषयलाई सम्बोधन गर्दै साइबर सुरक्षा निकाय स्थापना तथा साइबर आक्रमणको पहिचान, रोकथाम, प्रतिरक्षालगायतका आयामहरूको प्रभावकारीरूपमा सम्बोधन गर्ने, साइबर सुरक्षासम्बन्धी क्षमता अभिवृद्धि कार्यक्रम सञ्चालन गर्ने, आपत्कालीन कम्प्युटर उद्धार समूह (Computer Emergency Response Team) स्थापना गरी साइबर सुरक्षासम्बन्धी चुनौतीहरु शीघ्र सम्बोधन गर्ने व्यवस्था मिलाइने उल्लेख छ । राष्ट्रिय सुरक्षा नीति, २०७५ ले साइबर सुरक्षालाई राष्ट्रिय सुरक्षाको एक महत्वपूर्ण आयामका रूपमा समेटेको छ ।

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 छ । उक्त निर्देशिकामा व्यवस्था भएअनुरूप राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह (National Information Technology Emergency Response Team) र राष्ट्रिय साइबर सुरक्षा अनुगमन केन्द्र स्थापना भइ सरकारी सूचना प्रविधि प्रणालीहरूको निरन्तर अनुगमन भइरहेको छ ।

चालु आवधिक योजनाले साइबर सुरक्षा तथा गोपनीयतासम्बन्धी कार्य गर्न साइबर सुरक्षा अनुगमन केन्द्र स्थापना गरी साइबर सुरक्षालाई प्रभावकारी बनाइने विषयलाई जोड दिएको छ । डिजिटल नेपाल फ्रेमवर्क,

१ सूचना प्रविधि नीति, २०६७ ।

२ नेपालको संविधानको धारा ५१(च)(५) ।

३ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ ।

२०७६ मा राष्ट्रिय साइबर सुरक्षा केन्द्र स्थापनालगायतका साइबर सुरक्षासँग सम्बन्धित विषयहरूलाई समावेश गरिएको छ । दूरसञ्चार तथा इनटरनेट सेवा प्रदायकहरूको सूचना प्रविधि प्रणाली समेटिने गरी साइबर सुरक्षा विनियमावली, २०७७ कार्यान्वयनमा छ । सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१ साथै अनलाइन बाल सुरक्षा निर्देशिका, २०७६ कार्यान्वयनमा छन् । नेपाल सरकारको वार्षिक नीति तथा कार्यक्रममा साइबर सुरक्षासम्बन्धी विषयलाई प्राथमिकताका साथ उल्लेख गरेको पाइन्छ ।[४]

राष्ट्रिय साइबर सुरक्षा नीति, २०८० ले उठान गरेका विषय

नेपालको सन्दर्भमा राष्ट्रिय साइबर सुरक्षा नीतिका रूपमा पारित भएको यो पहिलो साइबर सुरक्षा नीति हो । यसले आगामी दिनमा साइबर सुरक्षा सम्बन्धमा निर्माण हुने कानुनहरूका सन्दर्भमा मार्ग निर्देशकका रूपमा काम गर्छ । हाल जारी राष्ट्रिय साइबर सुरक्षा नीति, २०८० को सन्दर्भमा व्यापकरूपमा छलफल गरी यसमा भएका कमजोरी औल्याएको खण्डमा आगामी दिनमा कानुन निर्माणका सन्दर्भमा यो नीतिले सार्थकता पाउन सक्छ ।

नेपालको सन्दर्भमा साइबर सुरक्षाका लागि प्रभावकारी कानूनी व्यवस्था तथा संस्थागत संरचना नहुनु, साइबर सुरक्षासम्बन्धी भौतिक तथा प्राविधिक पूर्वाधारको कमी, साइबर सुरक्षाका क्षेत्रमा दक्ष जनशक्ति तथा अनुसन्धानको कमी, साइबर सुरक्षासम्बन्धी सचेतनाको कमी, साइबर सुरक्षा सम्बन्धमा आन्तरिक तथा बाह्य समन्वयमा कमी जस्ता पक्षलाई समस्याका रूपमा राष्ट्रिय साइबर सुरक्षा नीतिले उल्लेख गरेको छ । यसका साथै सूचना तथा सञ्चार प्रविधि प्रणालीमा हुने साइबर आक्रमणको जोखिम न्यून गर्नका लागि नीतिगत र संरचनागत व्यवस्था गर्नु, साइबर सुरक्षा सुनिश्चित गर्न समयानुकूल अनुसन्धान र क्षमतामा आधारित दक्ष जनशक्ति विकास र उपयोग गर्नु, राष्ट्रिय संवेदनशील पूर्वाधार (National Critical Infrastructure) को पहिचान एवम् संरक्षण गर्नु, सार्वजनिक, व्यावसायिक र व्यक्तिगत सूचना तथा तथ्याङ्कमा अनधिकृत पहुँच नियन्त्रण गर्नु, नागरिक सेवामा विश्वसनीय डिजिटल प्रणाली र साइबर सुरक्षा प्रत्याभूत गर्नु, साइबर सुरक्षाका लागि राष्ट्रिय तथा अन्तर्राष्ट्रिय सहयोग तथा समन्वय गर्नुलाई नीतिले प्रमुख चुनौतीका रूपमा औल्याएको छ ।

नीतिको आवश्यकता

सञ्चार तथा सूचना प्रविधिको क्षेत्रमा भएको तीव्र विकासले विश्वलाई एक गाउँ (Global Village) का रूपमा परिणत गरेकाले सूचना प्रविधिको उच्चतम प्रयोग गरी आर्थिक तथा सामाजिक रूपान्तरणका लक्ष्य प्राप्त गर्न तथा साइबर सुरक्षामा सक्षम हुन विद्यमान नीतिगत तथा संस्थागत क्षमता अभिवृद्धि गर्नुपर्ने देखिएको छ । साइबर सुरक्षासम्बन्धी विषय नयाँ हुनुको साथै जटिल र चुनौतीपूर्णसमेत छ । नेपालमा यस क्षेत्रमा आवश्यक पर्ने अनुसन्धान र क्षमतामा आधारित दक्ष जनशक्तिको कमी छ । साइबर सुरक्षा, बौद्धिक सम्पत्तिको संरक्षण, सुरक्षा संवेदनशीलता र अभिसरण (Convergence) लगायतका विषय सम्बोधन गर्नुपर्ने देखिएको छ । साइबर आक्रमण एवम् साइबर अपराध सीमाबिहीन हुने भएकाले यसको नियन्त्रणका लागि अन्तर्राष्ट्रियस्तरमा सहयोग, समन्वय र सहकार्य आवश्यक देखिएको छ ।

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

यसैगरी सुरक्षित एवम् उत्थानशील साइबर स्पेस (Resilient Cyber Space) निर्माण गर्नु यस नीतिको दीर्घकालीन सोच देखिन्छ भने कानुनी र संस्थागत

४ राष्ट्रिय साइबर सुरक्षा नीति, २०८० ।

संरचना निर्माण, जनचेतना अभिवृद्धि र क्षमता विकास गर्दै विधि, प्रविधि र जनशक्तिको संयोजनबाट सूचना तथा तथ्याङ्क एवम् सूचना तथा सञ्चार प्रविधि प्रणालीलाई सुरक्षित बनाउने मुख्य ध्येय छ ।

लक्ष्य तथा उद्देश्य

विश्वव्यापी साइबर सुरक्षा सूचकाङ्क (Global Cyber Security Index–GCI) स्कोर (Score) ४४.९९ बाट आगामी ५ वर्षभित्र ६०, १० वर्षभित्र ७० र १५ वर्षभित्र ८० प्रतिशत पुऱ्याउने लक्ष्यसहित सुरक्षित साइबर स्पेस निर्माणका लागि कानुनी र संस्थागत व्यवस्था गर्नु, साइबर आक्रमणको जोखिम न्यूनीकरण गर्दै संवेदनशील राष्ट्रिय पूर्वाधार संरक्षण गर्नु, साइबर स्पेसलाई सशक्त र सुदृढ बनाउन साइबर सुरक्षा क्षेत्रमा अनुसन्धान, जनशक्ति उत्पादन एवम् कार्यरत जनशक्तिको क्षमता अभिवृद्धि गर्नु, डिजिटल प्रणालीबाट प्रवाह हुने सेवालाई विश्वसनीय र सुरक्षित बनाउनु, साइबर सुरक्षासम्बन्धी जोखिम न्यूनीकरणका लागि द्विपक्षीय, क्षेत्रीय तथा अन्तर्राष्ट्रिय स्तरमा समन्वय, अनुभव एवम् सहयोग आदान-प्रदान गर्नु यस नीतिको उद्देश्य छ ।

राष्ट्रिय साइबर सुरक्षा नीति, २०८० को रणनीति र कार्यनीतिहरू

क्र.स.	रणनीति	कार्यनीति
१.	सुरक्षित र उत्थानशील साइबर स्पेस बनाउन आवश्यक कानुन एवम् मापदण्ड तर्जुमा गर्ने ।	• विद्यमान कानुनलाई साइबर सुरक्षा अनुकूल हुनेगरी संशोधन, परिमार्जन र पुनरावलोकन गरिनेछ । • साइबर अपराध (Cybercrime) नियन्त्रण एवम् साइबर सुरक्षा सबलीकरणका लागि कानुन तर्जुमा गरिनेछ । • सूचना प्रविधिबाट सिर्जना हुने तथ्याङ्कहरु वर्गीकरण गर्नका लागि आवश्यक मापदण्ड निर्धारण गर्न कानुनी तथा नीतिगत व्यवस्था गरिनेछ । • साइबर अपराध अनुसन्धान, प्रमाण सङ्कलन, अभियोजन तथा नियन्त्रणका लागि अन्तर्राष्ट्रिय मापदण्डअनुरूप कानुनी तथा नीतिगत व्यवस्था गरिनेछ । • सूचनाको हक, गोपनीयताको हकलगायतका मौलिक अधिकारहरु संरक्षणका सन्दर्भमा राष्ट्रिय, क्षेत्रीय र अन्तर्राष्ट्रिय मापदण्डअनुरूप कानुनी तथा नीतिगत व्यवस्था गरिनेछ । • सूचना प्रविधिको माध्यमबाट सिर्जना हुने बौद्धिक सम्पत्ति तथा प्रतिलिपि अधिकार संरक्षणका लागि सम्बन्धित कानुनमा संशोधन र एकीकरण गरिनेछ । • साइबर आक्रमण तथा अपराधबाट सिर्जना हुने जोखिम बहन गर्न साइबर सुरक्षा बिमा व्यवस्था गरिनेछ । • साइबर सुरक्षाका मापदण्डहरु कार्यान्वयनका लागि अन्तर्राष्ट्रिय मापदण्डसमेतका आधारमा राष्ट्रिय साइबर सुरक्षा फ्रेमवर्क तर्जुमा गरिनेछ । • संवेदनशील पूर्वाधार जोखिम आकलन तथा न्यूनीकरण (Risk assessment and Mitigation) एवम् घटना प्रतिकार्य योजनाहरु (Incident Response Plans) निर्माण गरी कार्यान्वयन गरिनेछ । • व्यवसाय निरन्तरता योजना (Business Continuity Plan) तथा विपद् पुनर्लाभ योजना (Disaster Recovery Plan) बनाइ कार्यान्वयन गरिनेछ । • साइबर सुरक्षा प्रक्रियामा पूर्वतयारी, संरक्षण, पहिचान, प्रतिकार्य तथा पुनर्लाभ (Preparedness, Protection, Detection, Response and Recovery) सम्बन्धी कार्यविधि तयार गरी कार्यान्वयन गरिनेछ ।

		• राष्ट्रिय साइबर सुरक्षा रणनीतिका लागि प्राविधिक मार्गदर्शन (Technical Guideline) विकास गरिनेछ । • गुणस्तरीय सफ्टवेयर, हार्डवेयर नेटवर्क डिभाइस निर्माण, आयात प्रयोगसम्बन्धी मापदण्ड तयार गरी लागु गरिनेछ । • सञ्चार तथा सूचना प्रविधिसँग सम्बन्धित संस्थाहरुको अभिलेखीकरण (Profiling), इजाजतपत्र प्रदान (Licensing) तथा सफ्टवेयरहरु परीक्षण (Vetting) गरिने व्यवस्था गरिनेछ । • साइबर सुरक्षासम्बन्धी अन्तर्राष्ट्रिय अभ्याससमेतका आधारमा न्यूनतम प्राविधिक मापदण्ड (Minimum Technical Standard) निर्माण गरिनेछ । • साइबर सुरक्षा परीक्षणको मापदण्ड र परीक्षक (Auditor) को योग्यता निर्धारण गरिनेछ । • विभिन्न सूचना प्रविधि प्रणाली तथा सेवाबीच अन्तरसञ्चालन र डाटा आदान-प्रदानलाई सहज बनाउन खुला मापदण्डको प्रयोगलाई प्रोत्साहन गरिनेछ । • सूचना प्रविधि प्रणाली तथा सेवाबीच डाटा आदान-प्रदान गर्दा Encryption को प्रयोगलाई कार्यान्वयनमा ल्याइनेछ । • सूचना तथा सञ्चार प्रविधि र साइबर सुरक्षासम्बन्धी परामर्श सेवा तथा प्राविधिक उपकरण खरिदका लागि विशेष कानुनी व्यवस्था गरी कार्यान्वयन गरिनेछ । • डाटा केन्द्रको सुरक्षाका लागि आवश्यक मापदण्ड निर्माण गरिनेछ ।
२.	सूचना एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको सुरक्षा गर्न संस्थागत संरचनाहरु निर्माण एवम् सुदृढीकरण गर्ने ।	• साइबर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्धन, जनचेतना अभिवृद्धि, साइबर सुरक्षासम्बन्धी पूर्वतयारी, रोकथाम, पहिचान, प्रतिकार्य तथा पुनर्लाभ गर्न चौबीसै घण्टा (२४/७) सम्पर्क निकायका रुपमा कार्य गर्न, डिजिटल फोरेन्सिक अनुसन्धान गर्न तथा साइबर सुरक्षासँग सम्बन्धित निकायको नियमनकारी संस्थाका रुपमा समेत कार्य गर्ने गरी राष्ट्रिय साइबर सुरक्षा केन्द्र स्थापना गरिनेछ । • सूचना प्रविधि क्षेत्रको प्रवर्धन, नियमन तथा सरकारी निकायहरुका लागि आवश्यक पर्ने सूचना प्रविधि प्रणालीको विकास एवम् नियमन गर्ने गरी सूचना प्रविधि विभागको कार्यक्षेत्र विस्तार गरिनेछ । • साइबर सुरक्षा र साइबर अपराध अनुसन्धानसम्बन्धी विद्यमान संस्थाहरुको क्षमता अभिवृद्धि गरिनेछ । • साइबर सुरक्षासम्बन्धी आक्रमणहरुका बारेमा सूचना आदान-प्रदान गर्न डिजिटल पूर्वाधार (Digital Infrastructure) विकास गरिनेछ । • सरकारी नेटवर्क (Government Owned Network–Intranet) र National Internet Gateway निर्माण गरिनेछ । • साइबर सुरक्षासम्बन्धी राष्ट्रिय आकस्मिक योजना (National Contingency Plan) तयार गरी कार्यान्वयन गरिनेछ । • साइबर सुरक्षासम्बन्धी क्रियाकलापको समन्वय एवम् प्राथमिकीकरणका लागि राष्ट्रिय साइबर सुरक्षा कार्यान्वयन समिति गठन गरी क्रियाशील बनाइनेछ ।

		• नेपाल कम्प्युटर आकस्मिक सहायता समूह (Nepal Computer Emergency Response Team (NP–CERT)) तथा क्षेत्रगत कम्प्युटर आकस्मिक सहायता समूह र प्रदेशमा प्रादेशिक कम्प्युटर आकस्मिक सहायता समूह गठन गरी क्रियाशील तुल्याइनेछ । साथै सङ्घ, प्रदेश र स्थानीय तहको समन्वय र सहकार्यका लागि साइबर सुरक्षा सूचना संयन्त्र निर्माण गरिनेछ । • सार्वजिनक निकाय तथा संस्थाहरूको व्यावसायिक योजनामा सूचना सुरक्षा नीतिहरु समावेश गर्न प्रोत्साहित गरिनेछ ।
३.	साइबर सुरक्षालाई सुदृढ गर्न सबल एवम् सुरक्षित प्रविधि, पूर्वाधार र प्रक्रियाको व्यवस्था गर्दै संवेदनशील राष्ट्रिय पूर्वाधारहरु पहिचान गरी संरक्षण गर्ने ।	• सूचना तथा सञ्चार प्रविधि प्रयोग हुने राष्ट्रिय संवेदनशील पूर्वाधारहरु (National Critical Infrastructures) पहिचान गरी संरक्षण गरिनेछ । • संवेदनशील तथ्याङ्क सङ्कलन, प्रशोधन, प्रयोग तथा भण्डारण गर्ने सार्वजनिक निकाय तथा निजी क्षेत्रका संस्थालाई आवधिकरूपमा साइबर सुरक्षा परीक्षण अनिवार्य गरिनेछ । • व्यक्तिको अनलाइन पहिचानको सुरक्षा एवम् डाटा सुरक्षासम्बन्धी व्यवस्था गरिनेछ । • व्यक्तिगत वा संस्थागत तथ्याङ्कहरु सङ्कलन, प्रशोधन, प्रयोग एवम् भण्डारण गर्ने निकायहरूमा भएका साइबर आक्रमण तथा प्रयोगकर्ताका डाटा हानि नोक्सानी, तथा चोरीसम्बन्धी सूचनाको प्रतिवेदन राष्ट्रिय साइबर सुरक्षा केन्द्रमा गर्नुपर्ने व्यवस्था गरिनेछ । • साइबर सुरक्षासम्बन्धी पूर्वाधार निर्माण तथा स्तरोन्नति गरिनेछ । • साइबर सुरक्षासम्बन्धी परीक्षण एवम् प्रमाणीकरणका लागि प्रचलित कानुन, मापदण्ड एवम् असल अभ्यासको अनुशरण गर्ने व्यवस्था मिलाइनेछ । • साइबर सुरक्षा विकासका सूचकहरु निर्माण गरी राष्ट्रिय साइबर सुरक्षा परिपक्वता (National Cyber Security Maturity) मापन गरिनेछ । • विद्युतीय माध्यमबाट प्रवाह हुने सेवा तथा डाटालाई सुरक्षित र भरपर्दो बनाइनेछ । • सरकारी निकायहरूको एप्लिकेसन सफ्टवेयर र इमेलमा विद्युतीय हस्ताक्षरको प्रयोगलाई प्रोत्साहन गरिनेछ । • सार्वजनिक तथा सेवाप्रदायक निकायले प्रयोग गर्ने हार्डवेयर, सफ्टवेयर र नेटवर्कहरूको नियमित सुरक्षण परीक्षण गर्ने व्यवस्था मिलाइनेछ । • स्वदेशी सूचना तथा सञ्चार प्रविधिसम्बन्धी उत्पादनहरु खरिद तथा प्रयोगलाई प्रोत्साहित गरिनेछ । • सञ्चार तथा सूचना प्रविधि प्रणालीको सुदृढीकरण गर्न इथिकल ह्याकिङ (Ethical Hacking) लाई प्रोत्साहन गरिनेछ ।
४.	साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन अनुसन्धान र उपयोग गर्ने ।	• साइबर सुरक्षासम्बन्धी विषयलाई विद्यालय स्तर तथा उच्च शिक्षाको पाठ्यक्रममा समावेश गरिनेछ । • साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन गर्न साइबर सुरक्षाको क्षेत्रमा कार्य गर्ने सङ्घ/संस्थासँगको सहकार्यमा साइबर सुरक्षा फिनिसिङ स्कुल (Finishing School) को व्यवस्था गरिनेछ ।

		• राष्ट्रिय तथा अन्तर्राष्ट्रिय विश्वविद्यालयहरूसँगको सहकार्यमा साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन गरिनेछ । • साइबर सुरक्षासम्बन्धी अध्ययन/अनुसन्धान तथा विकासका लागि विश्वविद्यालयहरूलाई प्रोत्साहित गरिनेछ । • साइबर सुरक्षा क्षेत्रमा कार्यरत सार्वजनिक निकायका जनशक्तिको क्षमता अभिवृद्धिका लागि अन्तर्राष्ट्रिय मापदण्डअनुरूपका तालिम व्यवस्था गरिनेछ । • नेपाल कम्प्युटर आकस्मिक सहायता समूह (Nepal Computer Emergency Response Team (NP-CERT)) को क्षमता अभिवृद्धि गरिनेछ । • सरकारी निकायहरूमा आवश्यकताअनुसार साइबर सुरक्षासँग सम्बन्धित दक्ष जनशक्ति व्यवस्था गरिनेछ । • सार्वजनिक तथा निजी क्षेत्रका सूचना सुरक्षा पेसाकर्मीहरु (Information Security Professionals) को योग्यता पहिचान गरी नियमित क्षमता विकास गर्ने व्यवस्था गरिनेछ । • संवेदनशील सेवा प्रदायकहरु समेटिने गरी वार्षिकरूपमा राष्ट्रिय साइबर ड्रिल आयोजना गरिनेछ ।
५.	साइबर सुरक्षाका लागि डिजिटल साक्षरता कार्यक्रम सञ्चालनमा ल्याइ जनचेतना अभिवृद्धि गर्ने ।	• साइबर सुरक्षासम्बन्धी जनचेतना अभिवृद्धिका लागि स्थानीय तहमार्फत समुदाय परिचालन गरिनेछ । • साइबर सुरक्षाको जोखिमबाट सुरक्षित रहन सङ्घ, प्रदेश र स्थानीय तहसमेतको सहकार्यमा समुदायस्तरसम्म जनचेतना अभिवृद्धि कार्यक्रमहरु सञ्चालन गरिनेछ । • ज्येष्ठ नागरिक, महिला तथा बालबालिका, विशेष आवश्यकता भएका व्यक्तिहरु तथा नागरिक समाजलाई लक्षित गरी साइबर सुरक्षासम्बन्धी जनचेतना कार्यक्रमहरु सञ्चालन गरिनेछ । • साइबर सुरक्षासम्बन्धी सार्वजनिक चासोका विषय, घटना आदिबारे नागरिकलाई सुसूचित गर्न आवश्यकताअनुसार निर्देशन (Advisory) जारी गरिनेछ । • साइबर सुरक्षासम्बन्धी जनचेतनामूलक सामग्रीहरु निर्माण, वितरण र प्रसारण गरिनेछ ।
६.	सुरक्षित साइबर स्पेस निर्माणका लागि सार्वजनिक निकाय, निजी क्षेत्र र नागरिक समाजबीच समन्वय एवम् सहकार्य गर्ने ।	• सुरक्षित साइबर स्पेस निर्माणका लागि सम्पूर्ण समाज (Whole of the Society) को अवधारणा अवलम्बन गरिनेछ । • साइबर सुरक्षा पूर्वाधारहरु विकास गर्न सरकारी, निजी तथा सार्वजनिक निजी साझेदारी [Public-private partnership - (PPP) अवधारणा अवलम्बन गरिनेछ । • साइबर सुरक्षा जोखिम न्यूनीकरण गर्न नागरिक समाज, प्राज्ञिक संस्था तथा निजी क्षेत्रसँग सहकार्य एवम् समन्वय गरिनेछ । • साइबर सुरक्षासम्बन्धी कार्य गर्ने सङ्घ/संस्थाहरूलाई प्रोत्साहन एवम् नियमन गरिनेछ ।

७.	साइबर सुरक्षालाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय सङ्घ/संस्थाहरूसँग समन्वय एवम् सहकार्य गर्ने ।	• साइबर सुरक्षासम्बन्धी विषयमा अन्तर्राष्ट्रिय सहकार्यका लागि सम्पर्क विन्दु (Focal Point) तोकिनेछ । • साइबर सुरक्षाका लागि क्षमता अभिवृद्धि, सूचना आदान-प्रदान र साइबर अपराध नियन्त्रण गर्न द्विपक्षीय एवम् बहुपक्षीय सहकार्य गरिनेछ । • साइबर सुरक्षासम्बन्धी जोखिम न्यूनीकरण गर्न साइबर सुरक्षा क्षेत्रमा कार्यरत क्षेत्रीय एवम् अन्तर्राष्ट्रिय सङ्गठन तथा समूहहरूसँग मिलेर सहकार्य गरिनेछ । • साइबर सुरक्षासम्बन्धी जोखिम न्यूनीकरण गर्न साइबर सुरक्षा क्षेत्रमा कार्यरत क्षेत्रीय एवम् अन्तर्राष्ट्रिय संयन्त्रहरूमा सहभागिता जनाइनेछ ।
८.	साइबर सुरक्षाका लागि निरन्तर अनुगमन गरी सुरक्षित अनलाइन स्पेस निर्माण गर्ने ।	• इन्टरनेट तथा सामाजिक सञ्जाल प्रयोग गरी भ्रामक जानकारी सम्प्रेषण गर्ने कार्यलाई नियन्त्रण गरिनेछ । • महिला, बालबालिका वा लैङ्गिक तथा यौनिक अल्पसङ्ख्यक व्यक्तिविरुद्ध लक्षित अनलाइन सेवाहरूलाई निषेध गरिनेछ । • इन्टरनेट तथा सामाजिक सञ्जालको प्रयोगमार्फत हुने विभिन्न प्रकारका हिंसा एवम् भेदभाव नियन्त्रण गरिनेछ । • राष्ट्रिय सुरक्षामा आँच पुऱ्याउने, घृणा वा द्वेष फैलाउने, अनलाइन उत्पीडन (Online harassment) र साइबर बुलिङ गर्ने, सामाजिक तथा साम्प्रदायिक सद्भावमा खलल पुऱ्याउने, अश्लीलता फैलाउने किसिमका डिजिटल सामग्रीको सम्प्रेषण निषेध गरिनेछ । • स्पाम (Spam) मेसेजहरु सम्प्रेषण गर्ने कार्य नियन्त्रण गरिनेछ ।
९.	सफ्टवेयर विकासकर्ता वा आपूर्तिकर्ता, हार्डवेयर उत्पादक वा आपूर्तिकर्ता वा सेवा प्रदायकलाई आवश्यकताअनुसार जिम्मेवार बनाउने ।	• सफ्टवेयर विकासकर्तालाई आफूले विकास गरेको सफ्टवेयरको गुणस्तर एवम् सुरक्षा सुनिश्चितताका लागि जिम्मेवार बनाइनेछ । • हार्डवेयर निर्माणकर्तालाई आफूले निर्माण गरेको हार्डवेयरको गुणस्तर एवम् सुरक्षा सुनिश्चितताका लागि जिम्मेवार बनाइनेछ । • सूचना प्रविधिसम्बन्धी सेवा प्रदायकहरूलाई आफूले प्रदान गरेको सेवाको गुणस्तर एवम् सुरक्षा सुनिश्चितताका लागि जिम्मेवार बनाइनेछ । • आपूर्तिकर्तालाई आफूले आपूर्ति गरेको सफ्टवेयर तथा हार्डवेयरको गुणस्तर एवम् सुरक्षा सुनिश्चितताका लागि जिम्मेवार बनाइनेछ ।

यस नीति कार्यान्वयनमा नेतृत्वदायी भूमिका सञ्चार तथा सूचना प्रविधि मन्त्रालयको हुनेछ । क्षेत्रगत रणनीति एवम् कार्यनीतिहरूको प्रभावकारी कार्यान्वयन गर्ने जिम्मेवारी विषयगत मन्त्रालयहरूको रहने उल्लेख छ । यो नीति कार्यान्वयनका लागि सञ्चार तथा सूचना प्रविधि मन्त्री अध्यक्ष रहने गरी आवश्यक मार्गदर्शन गर्ने, नीतिअन्तर्गत सञ्चालन हुने कार्यक्रम तथा क्रियाकलापहरूको प्रभावकारी कार्यान्वयनमा समन्वय, सहजीकरण, अनुगमन तथा मूल्याङ्कन गर्ने गरी विभिन्न मन्त्रालय, राष्ट्र बैङ्क, विषयविज्ञसमेत रहेको निर्देशक समिति संस्थागत संरचनाका रूपमा व्यवस्था गरिएको छ ।

साइबर सुरक्षालाई मजबुत बनाउन राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूहका रूपमा समेत कार्य गर्नका लाग राष्ट्रिय साइबर सुरक्षा कार्यान्वयन समिति रहने व्यवस्था छ । सो समिति सञ्चार तथा सूचना प्रविधि मन्त्रालयका सहसचिव संयोजक रहने गरी विभिन्न मन्त्रालय, सुरक्षा निकाय, प्रेस काउन्सिल, विश्वविद्यालय तथा निजी क्षेत्रको समेत सहभागिता हुने गरी निर्माण हुने व्यवस्था छ । यो समितिले साइबर सुरक्षासम्बन्धी ऐन, नियम, नीति, रणनीति, मापदण्ड र कार्ययोजनामा समसामयिक सुधारका क्षेत्र पहिचान गर्ने, साइबर सुरक्षासम्बन्धी क्रियाकलापको समन्वय

एवम् प्राथमिकीकरण गर्ने, राष्ट्रिय संवेदनशील पूर्वाधार संरक्षणको निरीक्षण गर्ने, सूचना सुरक्षा पेसाकमीहरु (Information Security Professionals) का लागि आवश्यक न्यूनतम योग्यता पहिचान गर्ने, साइबर सुरक्षाका घटनाहरु विश्लेषण गर्ने, साइबर आक्रमणका सम्भावित जोखिमलाई ध्यान राखी चाल्नुपर्ने कदमहरु निर्धारण गर्ने, जोखिम आकलन एवम् आपत्कालीन योजनाहरु तथा सम्भाव्य जोखिम न्यूनीकरणका उपायहरु पहिचान गर्ने, साइबर सुरक्षा अनुसन्धान र दक्ष जनशक्ति निर्माणमा अन्य निकायसँग समन्वय गरी निर्देशक समितिमा पेस गर्ने जिम्मेवारी छ ।

साइबर सुरक्षा नीतिको लक्ष्य प्राप्तिका लागि राष्ट्रिय एवम् अन्तर्राष्ट्रिय स्रोत तथा साधन परिचालन गरी नीति कार्यान्वयनका लागि आवश्यक कानुन निर्माण एवम् विद्यमान कानुनहरु पुनरावलोकन गर्नेछ । नीतिको समीक्षा वार्षिकरुपमा गरी आवधिकरुपमा पुनरावलोकन गर्ने र नीति कार्यान्वयनका लागि अनुगमन गर्ने मुख्य जिम्मेवारी निर्देशक समितिलाई तोकेको छ । यो नीतिले सरोकारवालाहरुको सहयोग प्राप्त गर्न कठिन हुने सक्ने, संवेदनशील पूर्वाधार प्रदायकहरुले प्रदान गर्ने सेवाहरुको सुरक्षा र सूचना प्रणालीमा पहुँच पुऱ्याउन कठिन हुनुका साथै साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति व्यवस्थापनमा कठिनाइ हुन सक्ने पक्षलाई मुख्य चुनौतीका रुपमा लिएको पाइन्छ ।

नीतिबारे विश्लेषण

सूचना र प्रविधिमा भएको विकास साथसाथै यसको सुरक्षाको चुनौती समेत दिनानुदिन बढ्दै गइरहेको छ । औपचारिक रूपमा नेपाल सरकारकोतर्फबाट कुनै प्रकारको नीति पारित हुन नसकेको अवस्थामा आगामी दिनमा साइबर सुरक्षा सम्बन्धी कानुन तथा हाम्रो दृष्टिकोण के हुने भन्ने सन्दर्भमा राष्ट्रिय साइबर सुरक्षा नीति, २०८० पारित हुनु आफैमा महत्वपूर्ण कार्य हो । सूचना प्रविधिको उच्चतम प्रयोग गरी आर्थिक तथा सामाजिक रुपान्तरणका लक्ष्य प्राप्त गर्न तथा साइबर सुरक्षामा सक्षम हुन विद्यमान नीतिगत तथा संस्थागत क्षमता अभिवृद्धिको प्रयास गर्नु, साइबर सुरक्षा, बौद्धिक सम्पत्तिको संरक्षण, सुरक्षा संवेदनशीलता लगायतका विषयलाई सम्बोधन गर्नको लागि पाइला चाल्नुलाई सकारात्मक रूपमा लिन सकिन्छ । साथै सुरक्षित एवम् उत्थानशील साइबर स्पेस निर्माण गर्ने दीर्घकालीन सोच हुनु, कानुनी र संस्थागत संरचना निर्माण, जनचेतना अभिवृद्धि र क्षमता विकास गर्दै विधि, प्रविधि र जनशक्तिको संयोजनबाट सूचना तथा तथ्याङ्क एवम् सूचना तथा सञ्चार प्रविधि प्रणालीलाई सुरक्षित बनाउनेतर्फ चालेका पाइला यो नीतिको राम्रा पक्ष हुन् ।

अबको देशको विकासको मानक भनेको विश्वव्यापी साइबर सुरक्षा सूचाङ्क (Global Cyber Security Index–GCI) समेत हो । यो नीतिले सो सूचाङ्कलाई हाल कायम रहेका स्कोर (Score) ४४.९९ बाट आगामी ५ वर्षभित्र ६०, १० वर्षभित्र ७० र १५ वर्षभित्र ८० प्रतिशत पुऱ्याउने लक्ष्य लिएको छ । यद्यपि यो लक्ष्य नेपालको लागि धेरै महत्वकांक्षी र चुनौतीपूर्ण छ । तरपनि यस खालको परिकल्पनालाई सकारात्मक रूपमा लिन सकिन्छ ।

यस नीतिमा रहेका सकारात्मक पक्ष हुँदाहुँदै पनि यो नीति अलि हतारमा ल्याइएको छ । समग्र सरोकारवाला पक्षहरूसँग वृहत छलफल गरी नल्याएकाले उनीहरू यो नीतिको हिस्सेदार हुन सकेको देखिदैन । सरकारले नीति ल्याइ हेरौ न भनी भै गरी ल्याएको जस्तो देखिन्छ । यो नीतिले समग्र साइबर सुरक्षाको आगामी नियमनको रूपरेखा कोर्ने हुँदा अलि बढी तयारी र सबैका साथ लिएर आउन सक्नु पर्थ्यो सो हुन सकेको देखिदैन । यो नीतिमा नेसनल इन्टरनेट गेटवे निर्माण गरिने उल्लेख छ । यसले गर्दा इन्टरनेटमा सरकारी अधिपत्य कायम हुन सक्छ । र, नियत सफा नभए यस प्रावधानको आडमा सरकारले जुनसुकै बेला इन्टर नेटमाथि नियन्त्रण गर्न सक्छ । हाम्रो राज्य व्यवस्थाका लोकतान्त्रिक मूल्य तथा मान्यताहरूको मूलमर्महरू यो नीतिको कारणले दिर्घकालीन रूपमा निस्तेज हुने त होइनन् भन्ने कुरामा शंका गर्न सकिने अवस्था छ ।

सूचना प्रविधिको बढ्दो प्रयोगलाई नियमनका नाममा नियन्त्रण गर्ने भन्दा यसको सही सदुपयोगलाई विशेष प्रोत्साहन गर्नुपर्ने हुन्छ । तर नीतिमा इन्टरनेटको प्रयोगलाई नै संकुचन गर्ने तथा मनोवैज्ञानिक रूपमा

लोकतान्त्रिक मूल्य र मान्यताहरूलाई नै बनाउने खालका प्रावधानहरूलाई जोड दिइएको छ । त्यसैगरी इन्टरनेट तथा साइबर स्पेसमा नागरिकको सूचनामाथि पहुँच राख्ने र त्यसमाथि निगरानी सक्ने बाटो खुल्ला गरिएको छ । यसबाट सूचनाको दुरूपयोग हुने मात्र नभइ नागरिकको गोपनियताको हक र संविधानले नै प्रत्याभूत गरेको अभिव्यक्ति स्वतन्त्रतामाथि नै आँच पुऱ्याउन सक्ने जोखिम पनि छ ।

सुझाव

- नेपाल सरकारका तर्फबाट साइबर सुरक्षाको सन्दर्भमा विगतमा नीति अगाडि बढाउन खोजिएको भए पनि पारित नभएको सन्दर्भमा साइबर सुरक्षाका लागि यो नीति जारी गरिनु आफैंमा महत्ववपूर्ण कदम हो । देशका लागि बन्ने साइबर सुरक्षासम्बन्धी कानुनलाई मार्गदर्शन प्रदान गर्ने हुँदा सरोकारवालहरूसँग पर्याप्त छलफल गरी सूचना र प्रविधिमा भइरहेको तीव्रतर विकासलाई समेट्ने गरी यो नीति आउनुपर्ने थियो तर नीति पर्याप्त छलफलबिना र समेट्नुपर्ने कतिपय पक्ष नसमेटी आएको देखिन्छ ।
- नेपालको संविधानले जनताको प्रतिस्पर्धात्मक बहुदलीय लोकतान्त्रिक शासन प्रणाली, नागरिक स्वतन्त्रता, मौलिक अधिकार, मानव अधिकार, बालिग मताधिकार, आवधिक निर्वाचन, पूर्ण प्रेस स्वतन्त्रता तथा स्वतन्त्र, निष्पक्ष र सक्षम न्यायपालिका र कानुनी राज्यको अवधारणालगायतका लोकतान्त्रिक मूल्य र मान्यतामा आधारित राज्यका स्वमा परिकल्पना गरेको छ । त्यसो हुँदा नेपाल सरकारबाट पारित हुने कुनै पनि कानुन, नियम, नीति तथा कार्यहरु लोकतान्त्रिक मूल्य र मान्यताको विपरित हुने गरी जारी र लागु हुनै सक्दैन । नागरिकले मनोवैज्ञानिकस्वमा समेत लोकतान्त्रिक मूल्य/मान्यताबाट विचलन हुनु भनेको लोकतान्त्रिक मूल्य/मान्यताबाट विमुख हुनु हो । यो नीतिमा उल्लिखित सरकारी नेटवर्क (Government Owned Network–Intranet) र National Internet Gateway निर्माण गरिने कुराले नेपालको संविधान तथा लोकतान्त्रिक मूल्य/मान्यतालाई नै समाप्त गरी एकाधिकार कायम गर्ने आशय झल्कन्छ जुन संविधान तथा लोकतान्त्रिक मूल्य/मान्यता विपरित छ ।
- अहिलेसम्म साइबर सुरक्षाका सन्दर्भमा कानुनी तथा संरचनागतस्वमाबाट समेटिएका विषय मनन गरी देखिएका समस्यालाई राम्रोसँग प्रक्षेपण गरी नीतिमा समेटिएको भए आगामी दिनमा कानुन तथा साइबर सुरक्षामा आइपर्ने समस्या निर्मूलीकरण गर्न मार्गदर्शन प्राप्त हुने थियो ।
- यो नीति आमजनताको सूचना एवम् तथ्याङ्कमा सहज पहुँचसँगै सार्वजनिक, व्यावसायिक र व्यक्तिका तथ्याङ्क एवम् सूचनाहरुमा अनधिकृत पहुँच नियन्त्रण गर्ने भन्दा नागरिकका सूचनामा राज्यले जसरी पनि पहुँच राख्नुपर्छ भन्ने मान्यताबाट निर्देशित देखिन्छ ।
- यो नीतिले प्रविधिमा भएको विकास र चुनौतीलाई कसरी समेट्ने भन्ने सन्दर्भमा स्पष्ट पार्न सकेको छैन ।
- साइबर सुरक्षाको आवश्यकता तत्कालीन भएको हुँदा नीतिमा परिकल्पना गरेको कार्य सम्पन्न गर्ने तत्कालीन स्वरेखा प्रस्तुत हुनुपर्नेमा तत्कालीन समस्या निराकरण गर्ने सन्दर्भमा नीति मौन छ । नीतिमा तत्काल कार्य प्रारम्भ हुने गरी व्यवस्था हुनुपर्ने देखिन्छ ।
- नीतिमा ९ वटा रणनीति पूरा गर्नका लागि ७२ वटा कार्यनीति समावेश छ । रणनीति र कार्यनीति हेर्दा तत्कालै पूरा गर्नुपर्नेखालका छन् तर उल्लिखित रणनीति र कार्यनीति पूरा गर्ने कुनै ठोस परिकल्पना भने पाइँदैन ।
- यो नीति विद्यमान सूचना प्रविधिमा भएको तीव्र विकासका कारण सबैमा सूचना र प्रविधिको सुरक्षित पहुँच पुऱ्याउने भन्दा बढी सूचना र प्रविधिको पहुँचमा भएका नागरिकको गोपनीयतामा पहुँच पुऱ्याउनका लागि जारी भएको जस्तो देखिन्छ । त्यो आशंकालाई मेटाउने गरी कार्य गर्न जरूरी देखिन्छ ।

सन्दर्भ सामग्री

१. नेपालको संविधान ।

२. महर्जन, हर्षमान र राज, योगेश । २०७२ ।
इन्टरनेटसम्बन्धी नेपाल नीति : एक टिप्पणी ।
मिडिया अध्ययन १० । देवराज हुमागाईं, प्रत्यूष वन्त,
शेखर पराजुली, हर्षमान महर्जन, अर्जुन पन्थी,
सं, पृ.११९-१४० । काठमाडौं : मार्टिन चौतारी ।

३. राष्ट्रिय साइबर सुरक्षा नीति, २०८० ।

४. राष्ट्रिय सुरक्षा नीति, २०७३ ।

५. विद्यमान साइबर सुरक्षाका चुनौतीहरु एवम् साइबर
अपराध नियन्त्रणलाई प्रभावकारी बनाउने उपायका
सम्बन्धमा प्रतिवेदन पेस गर्न गठित अध्ययन
समितिको प्रतिविदन । २०७८ ।

६. राष्ट्रिय साइबर सुरक्षा नीति, २०८० को प्रारम्भिक
विश्लेषण : नेसनल इन्टरनेट गेटवेका नाममा
नियन्त्रित इन्टरनेटतर्फको यात्रा । काठमाडौं :
डिजिटल राइट नेपाल ।

७. सूचना प्रविधि नीति, २०६७ ।

८. सूचना प्रविधि नीति, २०५७ ।

सेन्टर फर मिडिया रिसर्च-नेपाल, मिडिया र नागरिक समाजसँग सम्बन्धित नीतिगत तथा व्यवहारिक पक्षमा अध्ययन तथा अनुसन्धान गर्ने संस्था हो । सेन्टरले मिडिया र नागरिक समाजका विभिन्न पक्षबारे अनुगमन, छलफल, तालिम, गोष्ठी, सेमिनारलगायत कार्य गर्दै आएको छ । सेन्टरले पछिल्लो समय सङ्घीय, प्रादेशिक र स्थानीय सरकारले निर्माण गरेका मिडिया र नागरिक समाजको क्षेत्रलाई संकुचन गर्ने गरी ल्याइएको नीति तथा कानुनहरुका कमी/कमजोरी केलाएर संशोधनका लागि टिप्पणी तथा सुझाव दिँदै आएको छ । समग्रमा, मिडिया एवं नागरिक समाजसँग सम्बन्धित नीतिबारे अध्ययन/अनुसन्धान गर्न चाहनेहरुको सहजता र नीति सम्बन्धमा सरोकारवालाहरुको सरोकार एवं कार्यलाई एकीकृत गरी नीतिलाई समयसापेक्ष र लोकतान्त्रिक बनाउन सहयोग गर्ने उद्देश्यले सेन्टरले नेपालः मिडिया पोलिसी हब र सिभिक स्पेश पोलिसी हब सञ्चालन गर्दै आएको छ ।

थप जानकारीका लागि:

सेन्टर फर मिडिया रिसर्च - नेपाल
पो.ब.नं. २४६२२, काठमाडौं, नेपाल
रूद्रमति मार्ग, अनामनगर, काठमाडौं ।
इमेलः cmrnepal@butmedia.org
वेभः research.butmedia.org