नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं

राष्ट्रिय साइबर सुरक्षा नीति, २०८०

१. पृष्ठभूमिः

सूचना प्रविधिमा भएको तीव्र विकाससँगै सामाजिक अन्तरक्रिया, सार्वजनिक सेवा एवम् सूचना प्रवाहमा आमूल परिवर्तन भइरहेको छ। सुरक्षित सूचना प्रविधिको प्रयोगबाट पारदर्शी एवम् प्रभावकारी सार्वजनिक सेवा 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 बनाई यसको प्रयोगमार्फत हुने सेवा प्रवाहमाथि जनताको विश्वास बढाउन आवश्यक देखिएको छ। राष्ट्रिय तथा अन्तर्राष्ट्रियस्तरबाट सूचना प्रविधि प्रणालीमाथि भइरहेका साइबर आक्रमणको प्रतिरक्षा सुनिश्चित गर्नुपर्ने भएको छ। नागरिक अधिकारका विश्वव्यापी मान्यता, नेपालको संविधान प्रदत्त मौलिक हकप्रतिको प्रतिबद्धतासमेतलाई कार्यान्वयन गर्न राष्ट्रिय साइबर सुरक्षा नीति आवश्यक छ। यस सन्दर्भमा सूचना प्रविधि प्रणालीमा साइबर आक्रमणबाट हुन सक्ने क्षतिलाई न्यूनीकरण गर्न र भविष्यमा हुन सक्ने 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 इलेक्ट्रोनिक 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 सम्बोधन गर्ने कुरामा जोड दिइएको छ। आवधिक योजनाहरूमा समेत साइबर सुरक्षाका विषयलाई जोड दिइएको छ। सार्वजनिक तथा निजी क्षेत्रसमेतबाट साइबर सुरक्षाका क्षेत्रमा केही कार्यहरू भइरहेका छन्।

३. वर्तमान स्थितिः

नेपालको संविधानमा राष्ट्रिय आवश्यकताअनुसार 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 गरिएको छ। विद्युतीय कारोबारलाई व्यवस्थित, सुरक्षित र भरपर्दो बनाउनुका साथै विद्युतीय अभिलेखमाथि अनधिकृत व्यक्तिको पहुँचलाई नियन्त्रण गर्ने उद्देश्यका साथ विद्युतीय कारोबार ऐन, २०६३ तथा विद्युतीय कारोबार नियमावली, २०६४ कार्यान्वयनमा रहेका छन्।

सूचना तथा सञ्चार प्रविधिको प्रयोगबाट सुशासन प्रवर्द्धन गर्नेलगायतका उद्देश्य राखी सूचना तथा सञ्चार प्रविधि नीति, २०७२ जारी भई कार्यान्वयनमा रहेको छ। यस नीतिमा साइबर सुरक्षाको विषयलाई सम्बोधन गर्दै साइबर सुरक्षा निकायको स्थापना तथा साइबर आक्रमणको पहिचान, रोकथाम, प्रतिरक्षालगायतका आयामहरूको प्रभावकारी रूपमा सम्बोधन गर्ने; साइबर सुरक्षासम्बन्धी क्षमता अभिवृद्धि कार्यक्रम सञ्चालन गर्ने; आपतकालीन कम्प्युटर उद्धार समूह (Computer Emergency Response Team) को स्थापना गरी साइबर सुरक्षासम्बन्धी चुनौतीहरू शीघ्र सम्बोधन गर्ने व्यवस्था मिलाइने उल्लेख गरिएको छ। राष्ट्रिय सुरक्षा नीति, २०७५ ले साइबर सुरक्षालाई राष्ट्रिय सुरक्षाको एक महत्त्वपूर्ण आयामको 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 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।

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, २०७६ मा राष्ट्रिय साइबर सुरक्षा केन्द्रको

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं

स्थापनालगायतका साइबर सुरक्षासँग सम्बन्धित विषयहरूलाई समावेश गरिएको छ। दूरसञ्चार तथा इन्टरनेट सेवा प्रदायकहरूको सूचना प्रविधि प्रणालीलाई समेटिने गरी साइबर सुरक्षा विनियमावली, २०७७ (Cyber Security Byelaw, 2020) कार्यान्वयनमा ल्याइएको छ। सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१ साथै अनलाइन बाल सुरक्षा निर्देशिका, २०७६ कार्यान्वयनमा रहेका छन्। नेपाल सरकारको वार्षिक नीति तथा कार्यक्रममा साइबर सुरक्षासम्बन्धी विषयलाई प्राथमिकताकासाथ उल्लेख गर्दै आएको छ।

४. समस्या तथा चुनौतीः

सूचना तथा सञ्चार प्रविधिको तीव्र विकास र व्यापकतासँगै यसको सुरक्षा चुनौती विश्वको प्रमुख चासोको विषय बन्दै गएको छ। सूचना तथा सञ्चार प्रविधि प्रणालीहरू माथिको साइबर आक्रमणको जोखिम दिनानुदिन बढ्दै गइरहेको छ। साइबर आक्रमण निश्चित भूगोलमा मात्र सीमित नभई विश्वव्यापी रूपमा भइरहेको छ। साइबरसँग सम्बन्धित अपराधिक गतिविधिहरूमा वृद्धि हुँदै गएकाले व्यक्तिगत तथा संस्थागत विवरणहरूको गोपनीयता एवम् तथ्याङ्कलगायत सूचना प्रविधि प्रणालीको सुरक्षा गर्ने कार्य जटिल बन्दै गएको छ। 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

(क) साइबर सुरक्षाको लागि प्रभावकारी कानूनी व्यवस्था तथा संस्थागत संरचना नहुनु,

(ख) साइबर सुरक्षासम्बन्धी भौतिक तथा प्राविधिक पूर्वाधारको कमी हुनु,

(ग) साइबर सुरक्षाको क्षेत्रमा दक्ष जनशक्ति तथा अनुसन्धानको कमी हुनु,

(घ) साइबर सुरक्षासम्बन्धी सचेतनाको कमी हुनु,

(ङ) साइबर सुरक्षा सम्बन्धमा आन्तरिक तथा बाह्य समन्वयमा कमी हुनु।

४.२ चुनौतीः

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

(ख) साइबर सुरक्षाको सुनिश्चितता गर्ने समयानुकूल अनुसन्धान र क्षमतामा आधारित दक्ष जनशक्तिको विकास र उपयोग गर्नु,

(ग) राष्ट्रिय संवेदनशील पूर्वाधार (National Critical Infrastructure) को पहिचान एवम् संरक्षण गर्नु,

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं

(घ) सार्वजनिक, व्यावसायिक र व्यक्तिगत सूचना तथा तथ्याङ्कमा अनधिकृत पहुँच नियन्त्रण गर्नु,

(ङ) नागरिक सेवामा विश्वसनीय डिजिटल प्रणाली र साइबर सुरक्षाको प्रत्याभूति गर्नु,

(च) साइबर सुरक्षाका लागि राष्ट्रिय तथा अन्तर्राष्ट्रिय सहयोग तथा समन्वय गर्नु।

५. नीतिको आवश्यकताः

सञ्चार तथा सूचना प्रविधिको क्षेत्रमा भएको तीव्र विकासले विश्वलाई एक गाउँ (Global Village) को 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 चुनौतीपूर्ण समेत रहेको छ। नेपालमा यस क्षेत्रमा आवश्यक पर्ने अनुसन्धान र क्षमतामा आधारित दक्ष जनशक्तिको कमी रहेको छ। साइबर सुरक्षा, बौद्धिक सम्पत्तिको संरक्षण, सुरक्षा संवेदनशीलता र अभिसरण (Convergence) लगायतका विषयहरू सम्बोधन गर्नुपर्ने देखिएको छ। साइबर आक्रमण एवम् साइबर अपराध सीमाविहीन हुने भएकोले यसको नियन्त्रणका लागि अन्तर्राष्ट्रियस्तरमा सहयोग, समन्वय र सहकार्य आवश्यक देखिएको छ।

यस नीतिले सङ्कलित, प्रशोधित, सङ्ग्रहित, प्रकाशित एवम् प्रसारित सूचना, तथ्याङ्क एवं सूचना तथा सञ्चार प्रविधि प्रणालीको गोपनीयता, अखण्डता, उपलब्धता, प्रामाणिकता 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 गर्नसमेत महत्त्वपूर्ण आधार निर्माण गर्ने हुँदा सुरक्षित एवम् उत्थानशील साइबरस्पेस निर्माणका लागि राष्ट्रिय साइबर सुरक्षा नीति तर्जुमा गर्न आवश्यक देखिएको छ।

६. दीर्घकालीन सोचः

सुरक्षित एवम् उत्थानशील साइबर स्पेस (Resilient Cyber Space) को निर्माण।

७. ध्येयः

कानूनी 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 बनाउने।

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं

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 अनुसन्धान, जनशक्ति उत्पादन एवम् कार्यरत जनशक्तिको क्षमता अभिवृद्धि गर्नु,

९.४ डिजिटल प्रणालीबाट प्रवाह हुने सेवालाई विश्वसनीय र सुरक्षित बनाउनु,

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

१०. **रणनीतिः**

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

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

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

१०.४ साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन अनुसन्धान र उपयोग गर्ने,

१०.५ साइबर सुरक्षाको लागि डिजिटल साक्षरता कार्यक्रम सञ्चालनमा ल्याई जनचेतना अभिवृद्धि गर्ने,

१०.६ सुरक्षित साइबर स्पेस निर्माणका लागि सार्वजनिक निकाय, निजी क्षेत्र र नागरिक समाजबीच समन्वय एवम् सहकार्य गर्ने,

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

१०.८ साइबर सुरक्षाका लागि निरन्तर अनुगमन गरी सुरक्षित अनलाइन स्पेस निर्माण गर्ने,

१०.९ सफ्टवेयर विकासकर्ता वा आपूर्तिकर्ता, हार्डवेयर उत्पादक वा आपूर्तिकर्ता वा सेवा प्रदायकलाई आवश्यकता अनुसार जिम्मेवार वनाउने।

नेपाल सरकार प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय सिंहदरवार, काठमाडौं

११. कार्यनीतिः

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

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

११.२ साइबर अपराध (Cybercrime) नियन्त्रण एवम् साइबर सुरक्षा सबलीकरणको लागि कानून तर्जुमा गरिनेछ।

११.३ सूचना प्रविधिबाट सिर्जना हुने तथ्याङ्कहरुको वर्गीकरण गर्नको लागि आवश्यक मापदण्ड निर्धारण गर्न कानूनी तथा नीतिगत व्यवस्था गरिनेछ।

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

११.५ सूचनाको हक, गोपनीयताको हकलगायतका मौलिक अधिकारहरूको संरक्षणका सन्दर्भमा राष्ट्रिय, क्षेत्रीय र अन्तर्राष्ट्रिय मापदण्डअनुरूप कानूनी तथा नीतिगत व्यवस्था गरिनेछ।

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

११.७ साइबर आक्रमण तथा अपराधबाट सिर्जना हुने जोखिम बहन गर्न साइबर सुरक्षा बिमाको व्यवस्था गरिनेछ।

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

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

११.१० व्यवसाय निरन्तरता योजना (Business Continuity Plan) तथा विपद् पुनर्लाभ योजना (Disaster Recovery Plan) बनाई कार्यान्वयन गरिनेछ।

११.११ साइबर सुरक्षा प्रक्रियामा पूर्वतयारी, संरक्षण, पहिचान, प्रतिकार्य तथा पुनर्लाभ (Preparedness, Protection, Detection, Response and Recovery) सम्बन्धी कार्यविधि तयार गरी कार्यान्वयन गरिनेछ।

११.१२ राष्ट्रिय साइबर सुरक्षा रणनीतिको लागि प्राविधिक मार्गदर्शन (Technical Guideline) को विकास गरिनेछ।

११.१३ गुणस्तरीय सफ्टवेयर, हार्डवेयर, नेटवर्क डिभाइसको निर्माण, आयात तथा प्रयोगसम्बन्धी मापदण्ड तयार गरी लागू गरिनेछ।

नेपाल सरकार प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय सिंहदरबार, काठमाडौं

११.१४ सञ्चार तथा सूचना प्रविधिसँग सम्बन्धित संस्थाहरूको अभिलेखीकरण (Profiling), इजाजतपत्र प्रदान (Licensing) तथा सफ्टवेयरहरूको परीक्षण (Vetting) गरिने व्यवस्था गरिनेछ।

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

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

११.१७ विभिन्न सूचना प्रविधि प्रणाली तथा सेवाबीच अन्तरसञ्चालन र डाटा आदानप्रदानलाई सहज बनाउन खुला मापदण्डको प्रयोगलाई प्रोत्साहन गरिनेछ।

११.१८ सूचना प्रविधि प्रणाली तथा सेवाबीच डाटा आदानप्रदान गर्दा Encryption को प्रयोगलाई कार्यान्वयनमा ल्याइनेछ।

११.१९ सूचना तथा सञ्चार प्रविधि र साइबर सुरक्षासम्बन्धी परामर्श सेवा तथा प्राविधिक उपकरण खरिदका लागि विशेष कानूनी व्यवस्था गरी कार्यान्वयन गरिनेछ।

११.२० डाटा केन्द्रको सुरक्षाका लागि आवश्यक मापदण्ड निर्माण गरिनेछ।

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

११.२१ साइबर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्द्धन, जनचेतना अभिवृद्धि, साइबर सुरक्षासम्बन्धी पूर्वतयारी, रोकथाम, पहिचान, प्रतिकार्य तथा पुनर्लाभ गर्न चौबिसै 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 साइबर सुरक्षा केन्द्र स्थापना गरिनेछ।

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

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

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

११.२५ सरकारी नेटवर्क (Government Owned Network-Intranet) र National Internet Gateway निर्माण गरिनेछ।

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

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं

११.२७ साइबर सुरक्षासम्बन्धी क्रियाकलापको समन्वय एवम् प्राथमिकीकरणका लागि राष्ट्रिय साइबर सुरक्षा कार्यान्वयन समिति गठन गरी क्रियाशील बनाईनेछ।

११.२८ नेपाल कम्प्यूटर आकस्मिक सहायता समूह (Nepal Computer Emergency Response Team (NP-CERT)) तथा क्षेत्रगत कम्प्युटर आकस्मिक सहायता समूह र प्रदेशमा प्रादेशिक कम्प्युटर आकस्मिक सहायता समूहको गठन गरी क्रियाशील तुल्याइनेछ। साथै संघ, प्रदेश र स्थानीय तहको समन्वय र सहकार्यका लागि साइबर सुरक्षा सूचना संयन्त्र निर्माण गरिनेछ।

११.२९ सार्वजिनक निकाय तथा संस्थाहरूको व्यावसायिक योजनामा सूचना सुरक्षा नीतिहरू समावेश गर्न प्रोत्साहित गरिनेछ।

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

११.३० सूचना तथा सञ्चार प्रविधि प्रयोग हुने राष्ट्रिय संवेदनशील पूर्वाधारहरू (National Critical Infrastructures) को पहिचान गरी संरक्षण गरिनेछ।

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

११.३२ व्यक्तिको अनलाइन पहिचानको सुरक्षा एवं डाटा सुरक्षासम्बन्धी व्यवस्था गरिनेछ।

११.३३ व्यक्तिगत वा संस्थागत तथ्याङ्कहरू 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।

११.३४ साइबर सुरक्षासम्बन्धी पूर्वाधारको निर्माण तथा स्तरोन्नति गरिनेछ।

११.३५ साइबर सुरक्षासम्बन्धी परीक्षण एवम् प्रमाणीकरणका लागि प्रचलित कानून, मापदण्ड एवम् असल अभ्यासको अनुशरण गर्ने व्यवस्था मिलाइनेछ।

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

११.३७ विद्युतीय माध्यमबाट प्रवाह हुने सेवा तथा डाटालाई सुरक्षित र भरपर्दो बनाइनेछ।

११.३८ सरकारी निकायहरूको एप्लिकेसन सफ्टवेयर र इमेलमा विद्युतीय हस्ताक्षरको प्रयोगलाई प्रोत्साहन गरिनेछ।

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं

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

११.४० स्वदेशी सूचना तथा सञ्चार प्रविधिसम्बन्धी उत्पादनहरू खरिद तथा प्रयोगलाई प्रोत्साहित गरिनेछ।

११.४१ सञ्चार तथा सूचना प्रविधि प्रणालीको सुदृढीकरण गर्न इथिकल ह्याकिङ (Ethical Hacking) लाई प्रोत्साहन गरिनेछ।

<u>रणनीति नं. १०.४ सँग सम्बन्धित</u> *(साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन, अनुसन्धान र उपयोग गर्ने।)*

११.४२ साइबर सुरक्षासम्बन्धी विषयलाई विद्यालयस्तर तथा उच्चशिक्षाको पाठ्यक्रममा समावेश गरिनेछ।

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

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

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

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

११.४७ नेपाल कम्प्युटर आकस्मिक सहायता समूह (Nepal Computer Emergency Response Team (NP-CERT)) को क्षमता अभिवृद्धि गरिनेछ।

११.४८ सरकारी निकायहरूमा आवश्यकताअनुसार साइबर सुरक्षासँग सम्बन्धित दक्ष जनशक्ति व्यवस्था गरिनेछ।

११.४९ सार्वजनिक तथा निजी क्षेत्रका सूचना सुरक्षा पेसाकर्मीहरू (Information Security Professionals) को योग्यता पहिचान गरी नियमित क्षमता विकास गर्ने व्यवस्था गरिनेछ।

११.५० संवेदनशील सेवा प्रदायकहरू समेटिने गरी वार्षिक रूपमा राष्ट्रिय साइबर ड्रिल आयोजना गरिनेछ।

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्‌को कार्यालय
सिंहदरबार, काठमाडौं

<u>रणनीति नं. १०.५ सँग सम्बन्धित</u> *(साइबर सुरक्षाको लागि डिजिटल साक्षारता कार्यक्रम सञ्चालनमा ल्याई जनचेतना अभिवृद्धि गर्ने।)*

११.५१ साइबर सुरक्षासम्बन्धी जनचेतना अभिवृद्धिका लागि स्थानीय तहमार्फत समुदायलाई परिचालन गरिनेछ।

११.५२ साइबर सुरक्षाको जोखिमबाट सुरक्षित रहन संघ, प्रदेश र स्थानीय तहसमेतको सहकार्यमा समुदायस्तरसम्म जनचेतना अभिवृद्धि कार्यक्रमहरू सञ्चालन गरिनेछ।

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

११.५४ साइबर सुरक्षासम्बन्धी सार्वजनिक चासोका विषय, घटना, आदिको बारेमा नागरिकलाई सुसूचित गर्न आवश्यकताअनुसार निर्देशन (Advisory) जारी गरिनेछ।

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

<u>रणनीति नं. १०.६ सँग सम्बन्धित</u> *(सुरक्षित साइबर स्पेस निर्माणका लागि सार्वजनिक निकाय, निजी क्षेत्र र नागरिक समाजबीच समन्वय एवम् सहकार्य गर्ने।)*

११.५६ सुरक्षित साइबर स्पेस निर्माणका लागि सम्पूर्ण समाज (Whole of the Society) को अवधारणालाई अवलम्बन गरिनेछ।

११.५७ साइबर सुरक्षा पूर्वाधारहरूको विकास गर्न सरकारी, निजी तथा सार्वजनिक निजी साझेदारी [Public–private partnership- (PPP)] अवधारणा अवलम्बन गरिनेछ।

११.५८ साइबर सुरक्षा जोखिमलाई न्यूनीकरण गर्न नागरिक समाज, प्राज्ञिक संस्था तथा निजी क्षेत्रसँग सहकार्य एवम् समन्वय गरिनेछ।

११.५९ साइबर सुरक्षासम्बन्धी कार्य गर्ने संघसंस्थाहरूलाई प्रोत्साहन एवम् नियमन गरिनेछ।

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

११.६० साइबर सुरक्षासम्बन्धी विषयमा अन्तर्राष्ट्रिय सहकार्यका लागि सम्पर्क विन्दु (Focal Point) तोकिनेछ।

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरवार, काठमाडौं

११.६१ साइबर सुरक्षाका लागि क्षमता अभिवृद्धि, सूचना आदानप्रदान र साइबर अपराध नियन्त्रण गर्न द्विपक्षीय एवम् बहुपक्षीय सहकार्य गरिनेछ।

११.६२ साइबर सुरक्षासम्बन्धी जोखिमलाई न्यूनीकरण गर्न साइबर सुरक्षा क्षेत्रमा कार्यरत क्षेत्रीय एवम् अन्तर्राष्ट्रिय संगठन तथा समूहहरूसँग आबद्ध भई सहकार्य गरिनेछ।

११.६३ साइबर सुरक्षासम्बन्धी जोखिमलाई न्यूनीकरण गर्न साइबर सुरक्षा क्षेत्रमा कार्यरत क्षेत्रीय एवम् अन्तर्राष्ट्रिय संयन्त्रहरुमा सहभागिता जनाइनेछ।

<u>रणनीति नं. १०.८ सँग सम्बन्धित</u> *(साइबर सुरक्षाका लागि निरन्तर अनुगमन गरी सुरक्षित अनलाइन स्पेस निर्माण गर्ने।)*

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

११.६५ महिला, बालबालिका वा लैङ्गिक तथा यौनिक अल्पसङ्ख्यक व्यक्तिका विरुद्ध लक्षित अनलाइन सेवाहरूलाई निषेध गरिनेछ।

११.६६ इन्टरनेट तथा सामाजिक सञ्जालको प्रयोगमार्फत हुने विभिन्न प्रकारका हिंसा एवम् भेदभावलाई नियन्त्रण गरिनेछ।

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

११.६८ स्पाम (Spam) मेसेजहरू सम्प्रेषण गर्ने कार्यलाई नियन्त्रण गरिनेछ।

<u>रणनीति नं. १०.९ सँग सम्बन्धित</u> *(सफ्टवेयर विकासकर्ता वा आपूर्तिकर्ता, हार्डवेयर उत्पादक वा आपूर्तिकर्ता वा सेवा प्रदायकलाई आवश्यकताअनुसार जिम्मेवार बनाउने।)*

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

११.७० हार्डवेयर निर्माणकर्तालाई आफूले निर्माण गरेको हार्डवेयरको गुणस्तर एवम् सुरक्षाको सुनिश्चितताका लागि जिम्मेवार बनाइनेछ।

११.७१ सूचना प्रविधिसम्बन्धी सेवा प्रदायकहरूलाई आफूले प्रदान गरेको सेवाको गुणस्तर एवम् सुरक्षाको सुनिश्चितताका लागि जिम्मेवार बनाइनेछ।

११.७२ आपूर्तिकर्तालाई आफूले आपूर्ति गरेको सफ्टवेयर तथा हार्डवेयरको गुणस्तर एवम् सुरक्षाको सुनिश्चितताका लागि जिम्मेवार बनाइनेछ।

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरवार, काठमाडौं

१२. संस्थागत व्यवस्थाः

१२.१ निर्देशक समिति

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, अर्थ मन्त्रालय	सदस्य
(ङ) सचिव, गृह मन्त्रालय	सदस्य
(च) सचिव, महिला, बालबालिका तथा ज्येष्ठ नागरिक मन्त्रालय	सदस्य
(छ) सचिव, रक्षा मन्त्रालय	सदस्य
(ज) सचिव, शिक्षा विज्ञान तथा प्रविधि मन्त्रालय	सदस्य
(झ) सचिव, सङ्घीय मामिला तथा सामान्य प्रशासन मन्त्रालय	सदस्य
(ञ) सचिव, सञ्चार तथा सूचना प्रविधि मन्त्रालय	सदस्य
(ट) नेपाल उद्योग वाणिज्य महासंघका अध्यक्ष	सदस्य
(ठ) मन्त्रालयले मनोनयन गरेको विषय विज्ञ प्रतिनिधि (१जना)	सदस्य
(ड) सहसचिव (सूचना प्रविधि महाशाखा), सञ्चार तथा सूचना प्रविधि मन्त्रालय	सदस्य सचिव

निर्देशक समितिको काम, कर्तव्य र अधिकार

(क) नीतिको प्रभावकारी कार्यान्वयनको लागि आवश्यक मार्गदर्शन गर्ने।

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

(ग) अन्य आवश्यक कार्यहरू गर्ने।

१२.२ राष्ट्रिय साइबर सुरक्षा कार्यान्वयन समिति :

(क) कार्यान्वयन समितिको संरचनाः

साइबर सुरक्षालाई मजबुत बनाउन राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूहको रूपमा समेत कार्य गर्न देहायको राष्ट्रिय साइबर सुरक्षा कार्यान्वयन समिति गठन गरिनेछ।

१) सहसचिव, सूचना प्रविधि महाशाखा, सञ्चार तथा सूचना प्रविधि मन्त्रालय	संयोजक

नेपाल सरकार प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय

२) महानिर्देशक, सूचना प्रविधि विभाग — सदस्य

३) नियन्त्रक, प्रमाणीकरण नियन्त्रकको कार्यालय — सदस्य

४) प्रमुख, एकीकृत सरकारी डाटा केन्द्र — सदस्य

५) निर्देशक, नेपाल दूरसञ्चार प्राधिकरण — सदस्य

६) निर्देशक(सूचना प्रविधि), नेपाल राष्ट्र बैङ्क — सदस्य

७) उपसचिव (सूचना प्रविधि), प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय — सदस्य

८) उपसचिव (सूचना प्रविधि), रक्षा मन्त्रालय — सदस्य

९) उपसचिव (सूचना प्रविधि), गृह मन्त्रालय — सदस्य

१०) प्रमुख सेनानी (सूचना प्रविधि), नेपाली सेना — सदस्य

११) प्रहरी उपरीक्षक (सूचना प्रविधि), नेपाल प्रहरी — सदस्य

१२) सशस्त्र प्रहरी उपरीक्षक (सूचना प्रविधि), सशस्त्र प्रहरी बल नेपाल — सदस्य

१३) उपअनुसन्धान निर्देशक (सूचना प्रविधि), राष्ट्रिय अनुसन्धान विभाग — सदस्य

१४) प्रतिनिधि, प्रेस काउन्सिल नेपाल — सदस्य

१५) विश्वविद्यालयका प्राज्ञिक/निजी क्षेत्र/क्यान महासंघ मध्येबाट मन्त्रालयले मनोनयन गरेको एक जना महिलासहित तीन जना विषय विज्ञ प्रतिनिधि — सदस्य

१६) प्रमुख, राष्ट्रिय साइबर सुरक्षा केन्द्र — सदस्य सचिव

(ख) कार्यान्वयन समितिको काम र कर्तव्यः

यस कार्यान्वयन समितिले देहायका कार्यहरू गरी निर्देशक 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) राष्ट्रिय संवेदनशील पूर्वाधार संरक्षणको निरीक्षण गर्ने।

४) सूचना सुरक्षा पेसाकर्मीहरू (Information Security Professionals) का लागि आवश्यक न्यूनतम योग्यताको पहिचान गर्ने।

५) साइबर सुरक्षाका घटनाहरूको विश्लेषण गर्ने।

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

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं

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

८) साइबर सुरक्षा अनुसन्धान र दक्ष जनशक्ति निर्माणमा अन्य निकायसँग समन्वय गर्ने।

१२.३ <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।

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

(क) नीति कार्यान्वयनको अनुगमन गर्ने मुख्य जिम्मेवारी निर्देशक समितिको हुनेछ।

(ख) यस नीतिको वार्षिक रूपमा समीक्षा गरी आवधिक रूपमा पुनरावलोकन गरिनेछ।

१६. जोखिमः

(क) सरोकारवालाको सहयोग प्राप्त गर्न कठिनाई 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।

नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं