Draft

राष्ट्रिय साइबर सुरक्षा नीति, २०७८

१. पृष्ठभूमिः

सूचना प्रविधिमा भएको तीव्र विकाससँगै सामाजिक अन्तरक्रिया, सार्वजनिक सेवा एवं सूचना प्रवाहमा आमूल परिवर्तन भएसँगै सूचना प्रविधिको प्रयोगबाट सुशासनको प्रत्याभूती र पारदर्शी एवं प्रभावकारी सार्वजनिक व्यवस्थापनको अपेक्षा गरिएको छ। सूचना प्रविधिको निरन्तर विकास, बढ्दो प्रयोग एवं गतिशिलतासंगै सूचना प्रविधि प्रणालीहरुमाथिको अनाधिकृत पहुँचको समस्या दिनानुदिन बढ्दै गैरहेको छ। राज्य व्यवस्थाको सञ्चालन, विकासको व्यवस्थापन, सार्वजनिक सेवा प्रवाह तथा जनताका दैनिक क्रियाकलापहरु सूचना प्रविधिमा निर्भर हुँदै गईरहेको अवस्थामा सूचना प्रविधि प्रणालीको सुरक्षा चुनौतिपूर्ण हुँदै गएको छ। राष्ट्रिय तथा अन्तर्राष्ट्रियस्तरमा सूचना प्रविधि प्रणालीमाथि भइरहेका साइवर आक्रमणको प्रतिरक्षा गर्ने विषयलाई सुनिश्चित गर्नु अत्यावश्यक भएको छ। सूचना प्रविधि प्रणालीमा साइवर आक्रमणबाट हुन सक्ने क्षतिलाई रोक्न, न्युनिकरण गर्न र भविष्यमा हुन सक्ने यस्ता आकमणहरुबाट सुरक्षित रहन साइवर सुरक्षा सम्बन्धी राष्ट्रिय नीति पहिलो पटक तर्जुमा गरिएको छ।

२. विगतको प्रयासः

नेपालमा वि.सं. २०२८ सालको राष्ट्रिय जनगणनाको तथ्याङ्क प्रशोधन क्रममा पहिलो पटक कम्प्युटर प्रविधिको प्रयोगबाट शुरु भएको सूचना प्रविधिको यात्रा हालसम्म आइपुग्दा सार्वजनिक, सामुदायिक तथा निजी क्षेत्रका अधिकांश कार्य तथा क्रियाकलापहरु सूचना प्रविधिमा निर्भर भएका देखिन्छन्। राष्ट्रिय सञ्चार नीति, २०४९, दूरसञ्चार ऐन, २०५३ र दूरसञ्चार नियमावली, २०५४ लागू भएपश्चात् मुलुकमा दूरसञ्चार क्षेत्र खुल्ला एवं प्रतिस्पर्धी युगमा प्रवेश गरेको हो। वि.सं. २०५७ मा लागू भएको सूचना प्रविधि नीतिले सूचना प्रविधिलाई देश विकासको वृहत्तर लक्ष्य हासिल गर्ने औजारको रुपमा स्थापित गर्ने अवधारणा अघि सारेको थियो। त्यसैगरी, सूचना प्रविधिको उपयोगबाट सामाजिक एवं आर्थिक विकासका लक्ष्यहरू हासिल गर्दै गरिवी न्यूनीकरण गर्ने लक्ष्यका साथ सूचना प्रविधि नीति, २०६७ जारी गरियो। उक्त नीतिमा सूचना प्रविधिको प्रयोगमा सूचना सुरक्षा एवम् तथ्याङ्क गोपनियतालाई सुदृढ गरिने विषयलाई जोड दिइएको थियो। सूचना तथा सञ्चार प्रविधि नीति, २०७२ मा सूचना प्रविधिको प्रयोगमा सुरक्षा एवं विश्वासको प्रत्याभूति गरिने, साइवर अपराधको

रोकथाम तथा अभियोजन प्रणालीको विकास गरिने, साइवर आक्रमण पहिचान, रोकथाम, प्रतिरक्षा लगायतका आयामहरुको प्रभावकारी सम्बोधन गर्ने कुरालाई जोड दिइएको छ। आवधिक योजनाहरुमा समेत साइवर सुरक्षाका विषयलाई जोड दिइएको पाइन्छ। विगतमा भएका प्रयासहरुबाट साइवर सुरक्षाका क्षेत्रमा केही कार्यहरु भएतापनि सूचना प्रविधिको बढ्दो प्रयोगसंगै साइवर सुरक्षामा नयाँ-नयाँ चुनौतिहरु देखापरेका छन्। बढ्दो साइवर आक्रमणको नियन्त्रण तथा सूचना प्रविधि प्रणाली सुरक्षाको लागि साइवर सुरक्षा सम्बन्धी छुट्टै नीतिको आवश्यकता देखिएको छ।

३. वर्तमान स्थितिः

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

त्यसैगरी, 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 सुनिश्चितता तथा ८० प्रतिशत नागरिक सेवाहरु अनलाइन मार्फत् प्रदान गरिने लक्ष्य लिएको छ। यस नीतिमा साइवर सुरक्षाको विषयलाई सम्बोधन गर्दै साइवर सुरक्षा निकाय स्थापना तथा साइवर आक्रमण पहिचान, रोकथाम, प्रतिरक्षा लगायतका आयामहरुको प्रभावकारी रुपमा सम्बोधन हुने व्यवस्था मिलाइने, साइवर सुरक्षा सम्बन्धी क्षमता अभिवृद्धि कार्यक्रम, आपतकालीन कम्प्युटर उद्दार समूह (Computer Emergency Response Team) को स्थापना गरी साइवर सुरक्षा सम्बन्धी चुनौतिहरु शीघ्र सम्बोधन गर्ने व्यवस्था मिलाइने उल्लेख गरिएको छ।

सूचना प्रविधिको विकास तथा बढ्दो प्रयोगसंगै 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 निर्देशिका अन्तर्गत राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह (National Information Technology Emergency Response Team) गठन हुनुको साथै

सोही निर्देशिकाले व्यवस्था गरे बमोजिम राष्ट्रिय साइवर सुरक्षा अनुगमन केन्द्र स्थापना भई सरकारी सूचना प्रविधि प्रणालीहरुको निरन्तर अनुगमन भइरहेको अवस्था छ।

चालू आवधिक योजनाले साईबर सुरक्षा तथा गोपनियता सम्वन्धी कार्य गर्न साईबर सुरक्षा अनुगमन केन्द्र स्थापना गरी साइवर सुरक्षालाई प्रभावकारी बनाइने विषयलाई जोड दिएको छ। डिजिटल नेपाल फ्रेमवर्क, २०७६ नेपाल सरकार (मन्त्रिपरिषद्) बाट स्वीकृत भई कार्यान्वयनमा रहेको छ। जसमा राष्ट्रिय साइवर सुरक्षा केन्द्रको स्थापना लगायतका साइवर सुरक्षासँग सम्बन्धित विषयहरुलाई समावेश गरिएको छ। आर्थिक वर्ष २०७७/७८ को बजेट वक्तव्यमा सार्वजनिक सेवा प्रवाहमा सूचना प्रविधिको प्रयोग बढाइने, साइवर सुरक्षा जोखिमको पहिचान, असर न्यूनीकरण र आकस्मिक साइवर सुरक्षा छरितो र भरपर्दो बनाउन साइवर फरेन्सिक ल्यावको स्तरोन्नती, छुट्टै साइवर सुरक्षा केन्द्र स्थापनाको लागि सम्भाव्यता अध्ययन लगायतका विषयहरु समावेश गरिएका छन्। चालू आर्थिक वर्षको नीति तथा कार्यक्रममा डिजिटल नेपाल फ्रेमवर्कको कार्यान्वयन गरी डिजिटल प्रविधिको उपयोगबाट सेवा प्रवाह, उत्पादकत्व र उत्पादन अभिवृद्धि गरी आर्थिक, सामाजिक रुपान्तरण गरिने तथा इन्टरनेट सेवालाई गुणस्तरीय र भरपर्दो बनाइने उल्लेख छ।

नेपाल दूरसञ्चार प्राधिकरणद्वारा दूरसञ्चार तथा इन्टरनेट सेवा प्रदायकहरुको सूचना प्रविधि प्रणालीलाई समेटिने गरी साइबर सुरक्षा विनियमावली, २०७७ (Cyber Security Byelaw, 2077) जारी गरी कार्यान्वयनमा रहेको छ।

साइवर सुरक्षाका क्षेत्रमा उल्लेखित व्यवस्था भएता पनि सूचना प्रविधिको बढ्दो प्रयोग एवं सूचना प्रविधिका प्रणालीहरुमाथि राष्ट्रिय एवं अन्तर्राष्ट्रियस्तरमा घटित साइवर आक्रमणका घटनाहरुले गर्दा अन्तर्राष्ट्रियस्तरमा समेत समन्वय र सहकार्य गर्ने गरी नयाँ साइवर सुरक्षा नीतिको तर्जुमा गर्न आवश्यक भएको छ।

४. समस्या र चुनौतिः

सूचना तथा सञ्चार प्रविधिको तीव्र विकास र व्यापकतासँगै यसको सुरक्षा चुनौती विश्वको प्रमुख चासोको विषय बन्दै गएको छ। सूचना प्रविधि प्रणालीहरुमाथिको साइवर आक्रमण दिनानुदिन बढ्दै गइरहेका छन्। साइबर आक्रमणहरू देश वा निश्चित भूगोलमा मात्र सीमित नभई विश्वव्यापीरुपमा अपराधीहरूले अति विज्ञता र सावधानीका साथ अपराधिक गतिविधिहरु

गरिरहेका कारण व्यक्तिगत तथा संस्थागत विवरणहरुको गोपनियता एवम् तथ्याङ्कहरुको सुरक्षा गर्ने कार्यमा जटिलता थपिंदै गएका छन्। विशेषगरी सूचना प्रविधि प्रणालीमाथि राष्ट्रिय एवम् अन्तराष्ट्रियस्तरबाट हुने यस प्रकारका अनाधिकृत पहुँचका प्रयासहरुले देहायका समस्या र चुनौतिहरु सिर्जना भएका छन्:

४.१ आम जनताको सूचना एवं तथ्याङ्कमा सहज पहुँच सँगै सार्वजनिक, व्यवसायिक र व्यक्तिका तथ्याङ्क एवम् सूचनाहरुमा अनाधिकृत पहुँच नियन्त्रण गर्ने।

४.२ सूचना प्रविधि प्रणालीमा हुने साइवर आक्रमणको जोखिम न्यूनीकरणका लागि संस्थागत र संरचनागत व्यवस्था गर्ने।

४.३ साइवर सुरक्षाको सुनिश्चितताको लागि दक्ष जनशक्ति विकास गर्ने।

४.४ साइवर सुरक्षाको विषयमा अन्तराष्ट्रिय संघ/संस्थासँग समन्वयन र सहकार्य गर्ने।

५. नयाँ नीतिको आवश्यकता:

विश्व एक गाउँ (Global Village) को रुपमा विकसित भईरहँदा सूचना प्रविधिको उच्चतम प्रयोग गरी आर्थिक तथा सामाजिक रुपान्तरणका लक्ष्यहरु प्राप्त गर्न विद्यमान नीतिगत तथा संस्थागत क्षमता अपर्याप्त देखिन्छ। साइबर सुरक्षामा मुलुकलाई सबल र सक्षम बनाउनका लागि आवश्यक पर्ने संस्थागत र संरचनागत व्यवस्था गर्नु अत्यावश्यक देखिएको छ। साइबर सुरक्षा हाम्रो सन्दर्भमा नयाँ हुनुको साथै विश्वको लागि जटिल र चुनौतिको विषय बन्दै गएको छ। यस क्षेत्रमा आवश्यक पर्ने दक्ष जनशक्तिको अभाव, अझ सार्वजनिक सेवामा यसको अभाव टड्कारो रुपमा देखिएको छ। बढ्दो साइबर आक्रमण नियन्त्रणका लागि अन्तर्राष्ट्रियस्तरमा सहयोग र सहकार्य गर्न सकिएमा मात्र अपेक्षित उपलब्धी हाँसिल गर्न सकिने अवस्था रहेको छ। साइबर सुरक्षा, बौद्धिक सम्पतिको संरक्षण, अन्तर क्षेत्रगत विषय सम्बोधन, सुरक्षा संवेदनशीलता र अभिसरण (Convergence) लगायतका विषयहरु सम्बोधन गरि प्रविधिमैत्री कार्यवातावरण निर्माण गर्न तथा बदलिदो परिवेश अनुरुप सूचना प्रविधिको उच्चतम प्रयोग गरी सुशासनको प्रवर्द्धन गर्न, साईबर सूरक्षा सम्बन्धी नीतिगत, संस्थागत, कार्यगत एवं प्रक्रियागत उपायहरु अवलम्वन गर्न आवश्यक भएकोले नयाँ साईबर सूरक्षा नीतिको आवश्यकता महसूस भएको छ। नयाँ नीतिले संकलित, प्रशोधित, सङ्ग्रहीत र प्रसारित डाटा तथा सूचना प्रणालीको गोपनियता, अखण्डता, उपलब्धता एवं प्रमाणिकता (Confidentiality, Integrity, Availability and Authenticity) को स्तरवृद्धि गर्न संवेदनशील पूर्वाधार प्रदायकहरूले सञ्चालन गरेको वा उपयोग गरेको सूचना प्रणालीको क्षमता वृद्धि गर्न महत्वपूर्ण आधार निर्माण गर्ने विश्वास लिइएको छ।

६. दीर्घकालीन सोचः

साइवर जोखिमलाई सम्बोधन गर्दै व्यक्ति, व्यवसाय एवं सरकारका लागि भरपर्दो, सुरक्षित एवं लचिलो साइबर स्पेश (Resilient Cyber Space) निर्माण गर्ने।

७. परिदृष्यः

सूचना एवं सूचना प्रविधि प्रणालीको सुरक्षा गर्न संस्थागत र कानूनी संरचना निर्माण एवं जनचेतना र क्षमता अभिवृद्धि गर्दै उपलब्ध विधि, प्रविधि र जनशक्तिको संयोजनबाट साइबरस्पेशमा हुन सक्ने सम्भावित क्षतिलाई न्यून गर्ने।

८. लक्ष्यः

८.१ आगामी तीन वर्षभित्रमा भरपर्दो, सुरक्षित एवं लचिलो साइवरस्पेस निर्माणका लागि कानूनी व्यवस्था गर्ने;

८.२ आगामी पाँच वर्षभित्रमा भरपर्दो, सुरक्षित एवं लचिलो साइवरस्पेस निर्माणका लागि संस्थागत र संगठनात्मक पूर्वाधार स्थापना गर्ने;

८.३ साइवर जोखिमलाई न्यूनीकरण गर्न जनचेतना वृद्धि एवम् दक्ष जनशक्ति उत्पादन गर्ने;

८.४ सम्भावित साइवर जोखिमबाट सुरक्षित रहन तथा जोखिमलाई न्यूनिकरण गर्न राष्ट्रिय तथा अन्तर्राष्ट्रिय समुदायसँग सहकार्य गर्ने।

९. उद्देश्यः

९.१ सुरक्षित, भरपर्दो र लचिलो साइवरस्पेस बनाउन एवं यस क्षेत्रमा अन्तर्राष्ट्रिय मापदण्ड/स्तर कायम गर्न कानूनी तथा नीतिगत व्यवस्थालाई सशक्त बनाउनु।

९.२ सूचना एवं सूचना प्रविधि प्रणालीको सुरक्षाको लागि संस्थागत र संगठनात्मक संरचनाहरू निर्माण गर्नु।

९.३ साइवरस्पेसलाई सशक्त र सुदृढ बनाउन साइवर सुरक्षाका विषयमा जनचेतना बढाउने तथा साइवर सुरक्षा क्षेत्रमा जनशक्ति उत्पादन एवम् कार्यरत जनशक्तिको क्षमता अभिवृद्धि गर्नु।

९.४ साइबर सुरक्षा सम्बन्धी विश्वव्यापी जोखिमलाई मध्यनजर गरी त्यस्ता जोखिमहरूका विरुद्ध द्विपक्षीय, क्षेत्रीय तथा अन्तर्राष्ट्रिय मुलुक एवम् संगठनहरुसँग सहकार्य गर्नु।

१०. रणनीतिः

१०.१ सुरक्षित, भरपर्दो र लचिलो साइवरस्पेस बनाउन आवश्यक कानून एवम् मापदण्डहरु निर्माण गरिने।

१०.२ सूचना एवं सूचना प्रविधि प्रणाली सुरक्षा गर्न अन्तर्राष्ट्रिय प्रचलन समेतको आधारमा संस्थागत एवं संगठनात्मक संरचनाहरू निर्माण एवम् सुदृढिकरण गरिने।

१०.३ साइबर सुरक्षालाई सुदृढ गर्न सबल एवम् सुरक्षित प्रविधि, पूर्वाधार र प्रकृयाको व्यवस्था गरिने।

१०.४ साइवर सुरक्षा सम्बन्धी दक्ष जनशक्ति उत्पादन गरिने।

१०.५ साइवर सुरक्षाको विषयमा जनचेतना अभिवृद्धि गरिने।

१०.६ सुरक्षित साइवरस्पेस निर्माणका लागि सार्वजनिक निकाय तथा निजी क्षेत्रसँग समन्वय एवम् सहकार्य गरिने।

१०.७ साइवर सुरक्षालाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय संघ-संगठनहरुसँग समन्वय एवम् सहकार्य गरिने।

१०.८ सुरक्षित अनलाइन स्पेस निर्माण गरिने।

११. कार्यनीतिः

रणनीति नं. १०.१ सँग सम्बन्धित *(सुरक्षित, भरपर्दो र लचिलो साइवरस्पेस बनाउन आवश्यक कानून एवम् मापदण्डहरु निर्माण गरिने।)*

११.१ विद्यमान कानूनलाई साइवर सुरक्षा अनुकूल हुने गरी संशोधन, परिमार्जन र पुनरावलोकन गरी समय सान्दर्भिक बनाईने।

११.२ साइबर अपराध (Cybercrime) एवं सूचना तथा सञ्चार प्रविधिको अपराधिक दुरुपयोग विरुद्ध एवं साइबर सुरक्षा सबलिकरणको लागि कानून निर्माण गरिने ।

११.३ अपराधिकरण, अनुसन्धान, विद्युत्तीय प्रमाण तथा अन्तर्राष्ट्रिय सहयोगका साथै मौलिक अधिकारहरूको संरक्षणका सन्दर्भमा क्षेत्रीय एवं अन्तर्राष्ट्रिय मापदण्ड अनुरुप कानूनी तथा नीतिगत व्यवस्था गरिने।

११.४ नागरिकहरूका संवेदनशिल तथ्यांकहरू संकलन, प्रशोधन, प्रयोग तथा भण्डारण गर्ने नीजि तथा सार्वजनिक निकायहरूलाई आवधिकरूपमा साइबर सुरक्षा परिक्षण अनिवार्य गर्ने व्यवस्था मिलाइने।

११.५ नेपाली नागरिकहरूको अनलाईन पहिचानको सुरक्षा तथा डाटा सुरक्षा सम्बन्धी उपायहरू अवलम्बन गरिने।

११.६ बौद्धिक सम्पत्ती तथा प्रतिलिपि अधिकार संरक्षणको व्यवस्था मिलाइने।

११.७ साइबर सुरक्षा सम्बन्धी अन्तर्राष्ट्रिय अभ्यास समेतका आधारमा न्यूनतम प्राविधिक मापदण्ड (Minimum Technical Standard) निर्माण गरिने।

११.८ साइबर सुरक्षाका मापदण्डहरू कार्यान्वयनका लागि अन्तर्राष्ट्रिय मापदण्ड समेतका आधारमा राष्ट्रिय साइबर सुरक्षा फ्रेमवर्क तर्जुमा गरिने।

११.९ गुणस्तरीय सफ्टवयर निर्माणका लागि आवश्यक पर्ने मापदण्ड तयार गरी लागु गरिने।

११.१० नेपाली नागरिकका गोपनीयताको हक, सूचनाको हक एवं स्वतन्त्रताको संरक्षण गर्न व्यक्तिगत एवं सामूहिक साइबर सुरक्षाका उपायहरु निर्धारण गरिने ।

११.११ व्यक्तिगत वा संस्थागत तथ्यांकहरू संकलन, प्रशोधन, प्रयोग एवं भण्डारण गर्ने निकायहरूमा भएका साइबर आक्रमण तथा प्रयोगकर्ताका डाटा हानी, नोक्सानी, तथा चोरी सम्बन्धी सूचना सार्वजनिक गर्नुपर्ने व्यवस्था गरिने।

११.१२ संवेदनशील पूर्वाधार प्रदायकहरूसँग समन्वय गरी जोखिम निर्धारण तथा न्यूनीकरण (Risk assessment and Mitigation) एवं आपतकालीन प्रतिरक्षा योजनाहरू (Incident Response Plans)को निर्माण गरी कार्यान्वयन गरिने।

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

११.१४ राष्ट्रिय साइबर सुरक्षा रणनीतिको लागि प्राविधिक निर्देशिका (Technical guidelines) को विकास गरिने।

रणनीति नं. १०.२ सँग सम्बन्धित ***(सूचना एवं सूचना प्रविधि प्रणाली सुरक्षा गर्न अन्तर्राष्ट्रिय प्रचलन समेतको आधारमा संस्थागत एवं संगठनात्मक संरचनाहरू निर्माण एवम् सुदृढिकरण गरिने।)***

११.१५ साइवर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्धन, जनचेतना अभिवृद्धि, साइबर सुरक्षा सम्बन्धी तयारी, रोकथाम, पहिचान, प्रतिक्रिया तथा पुनर्लाभ गर्न, २४/७ सम्पर्क निकायको रुपमा कार्य गर्न तथा डिजिटल फोरेन्सिक अनुसन्धान गर्न राष्ट्रिय साईबर सुरक्षा केन्द्र स्थापना गरिने।

११.१६ साइबर सुरक्षा र साइबर अपराध अनुसन्धान सम्बन्धी विद्यमान संस्थाहरूको क्षमता अभिवृद्धि गरिने।

११.१७ साईबर सुरक्षा सम्बन्धी आक्रमणहरूका बारेमा अद्यावधिक सूचना आदानप्रदान गर्न डिजिटल पूर्वाधार (Digital Infrastructure) को विकास गरिने।

११.१८ राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूहको क्षमता अभिवृद्धि गरी साइबर सुरक्षा सम्बन्धी राष्ट्रिय आकस्मिक योजना (National Contingency Plan) तयार गरी कार्यान्वयन गरिने।

११.१९ साइबर सुरक्षासम्बन्धी अनुसन्धान तथा विकास क्रियाकलापको प्राथमिकीकरण र समन्वयका लागि राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह गठन गरी क्रियाशील बनाईने।

११.२० सरकारी निकायहरुका लागि आवश्यक पर्ने सूचना प्रविधि प्रणालि निर्माण, परिमार्जन, मर्मत् सम्भार एवं सोको सुरक्षण परीक्षणका लागि सूचना प्रविधि प्राधिकरणको स्थापना गरिने।

११.२१ क्षेत्रगत सूचना प्रविधि आकस्मिक सहायता समुहको गठन गरिने।

रणनीति नं. १०.३ सँग सम्बन्धित ***(साइबर सुरक्षालाई सुदृढ गर्न सबल एवम् सुरक्षित प्रविधि, पूर्वाधार र प्रकृयाको व्यवस्था गरिने)***

११.२२ सरकारी निकायहरुको एप्लिकेशन सफ्टवयर र ईमेलमा विद्युतीय हस्ताक्षरको प्रयोग अनिवार्य गर्ने व्यवस्था मिलाइने।

११.२३ राष्ट्रिय संवेदनशील पूर्वाधारहरु (National Critical Infrastructures) को पहिचान एवं संरक्षण गर्ने व्यवस्था गरिने।

११.२४ साइबर सुरक्षासम्बन्धी असल अभ्यास, मापदण्ड एवं निर्देशिका (जस्तैः ISO 27001) अनुरूप भए नभएको परीक्षण एवम् प्रमाणीकरणका लागि आवश्यक व्यवस्था गरिने।

११.२५ साइबर जोखिम तथा साइबर सुरक्षा विकासका सूचकहरूको प्रयोग गरी वार्षिकरुपमा राष्ट्रिय साइबर सुरक्षा सर्वेक्षण मार्फत राष्ट्रिय साइबर सुरक्षा परिपक्वता (National Cyber Security Maturity) मापन गरिने।

११.२६ विद्युतीय माध्यमबाट प्रवाह हुने सेवालाई सुरक्षित र भरपर्दो बनाइने ।

११.२७ विद्युतीय माध्यमबाट प्रवाह हुने सरकारी डाटा सुरक्षित र भरपर्दो बनाइने ।

११.२८ सरकारी निकायहरुले प्रयोग गर्ने सफ्टवयरहरुको नियमित सुरक्षण परीक्षण गरिने व्यवस्थालाई प्रभावकारी बनाइने।

रणनीति नं. १०.४ सँग सम्बन्धित ***(साइवर सुरक्षा सम्बन्धी दक्ष जनशक्ति उत्पादन गरिने।)***

११.२९ विश्वविद्यालयहरुसंगको सहकार्यमा साइबर सुरक्षा सम्बन्धी दक्ष जनशक्ति उत्पादन गरिने।

११.३० साइबर सुरक्षाको क्षेत्रमा दक्ष जनशक्ति उत्पादन गर्न साइबर सुरक्षा उद्योग समेतको सहकार्यमा सूचना प्रविधिमा स्नातक तह उत्तिर्ण गरेका विद्यार्थीहरूकोलागि साइबर सुरक्षा फिनिसिङ्ग स्कुल (Finishing School) को व्यवस्था गरिने।

११.३१ विद्यालयस्तरमा साइवर सुरक्षा सम्बन्धी जानकारी प्रदान गर्नका लागि विद्यालयस्तरको पाठ्यक्रममा साइवर सुरक्षा सम्बन्धी विषयलाई समावेश गरिने।

११.३२ साइबर सुरक्षाका नवीनतम प्रचलन सम्बन्धमा तालिम उपलब्ध गराउन पाठ्यक्रमको विकास गरिने।

११.३३ साइवर सुरक्षा क्षेत्रमा कार्यरत जनशक्तिको क्षमता अभिवृद्धिका लागि अन्तर्राष्ट्रिय मापदण्ड अनुरुपका तालिमको व्यवस्था गरिने।

११.३४ साइवर सुरक्षालाई विशिष्टीकृत सेवाको रुपमा स्थापित गर्न निजामती सेवामा छुट्टै साइवर सुरक्षा समूह स्थापना गरिने।

११.३५ सार्वजनिक क्षेत्रका सूचना सुरक्षा पेशाकर्मीहरू (Information Security professionals)को आवश्यक योग्यताको पहिचान गरि नियमित क्षमता विकास गरिने।

११.३६ वित्त, दूरसञ्चार, उर्जा, स्वास्थ्य लगायतका संवेदनशिल सेवा प्रदायकहरू समेटिने गरी वार्षिकरूपमा राष्ट्रिय साइबर ड्रिल गरिने।

रणनीति नं. १०.५ सँग सम्बन्धित ***(साइवर सुरक्षाको विषयमा जनचेतना अभिवृद्धि गरिने।)***

११.३७ समुदायमा साइबर सुरक्षा सम्बन्धी जनचेतना अभिवृद्धिका लागि सामुदायिक साइबर सुरक्षा सहायता समुह (Community CERT) गठन गरी परिचालन गरिने।

११.३८ साइवर सुरक्षाको जोखिमबाट सुरक्षित रहन जनचेतना अभिवृद्धि कार्यक्रमहरु सञ्चालन गरिने।

११.३९ ज्येष्ठ नागरिक, बालबालिका, विशेष आवश्यकता भएका व्यक्तिहरू तथा नागरिक समाजलाई लक्षित गरी साइबर हाइजिन सम्बन्धि कार्यक्रमहरू सञ्चालन गरिने।

११.४० साइबर सुरक्षा सम्बन्धी सार्वजनिक चासोका विषय, घटना, आदि को बारेमा नागरिकलाई सुसुचित गर्न आवश्यकता अनुसार परामर्श (Advisory) जारी गरिने।

११.४१ साइबर सुरक्षा सम्बन्धी जनचेतनामुलक सामाग्रीहरू निर्माण गरी वितरण गरिने।

रणनीति नं. १०.६ सँग सम्बन्धित ***(सुरक्षित साइवरस्पेस निर्माणका लागि निजी क्षेत्रसँग सहकार्य गरिने।)***

११.४२ साइबर सुरक्षा सम्बन्धी उद्योगलाई प्रोत्साहन गरिने।

११.४३ साइबर सुरक्षाको क्षेत्रमा कार्यरत उद्योगहरूको नियमनको व्यवस्था मिलाइने।

११.४४ निजि क्षेत्रमा साइबर सुरक्षा सम्बन्धी दक्षता अभिवृद्धिको लागि सहकार्य गरिने।

११.४५ सार्वजनिक निजी साझेदारी [Public–private partnership- (PPP)] को अवधारणा अनुरुप संयन्त्र निर्माण गरी पुर्वाधारहरुको विकास गरिने।

११.४६ साइवर जोखिमलाई न्यूनिकरण गर्न निजी क्षेत्रसँग सहकार्य गरिने।

रणनीति नं. १०.७ सँग सम्बन्धित ***(साइवर सुरक्षाको स्थितिलाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय संघ-संगठनहरुसँग समन्वय र सहकार्य गरिने।)***

११.४७ साईबर अपराध सम्बन्धि विषयमा अन्तर्राष्ट्रिय सहकार्यका लागि एकल विन्दु तोकिने।

११.४८ संयुक्त राष्ट्र संघीय महासभाका प्रस्तावहरूका साथै अन्तर्राष्ट्रिय दूरसञ्चार संघबाट लागू हुने सुझावहरूमा आधारित भई सूचना तथा सञ्चार प्रविधि (ICT) मा सुरक्षा तथा विश्वासको वातावरण सृजना गर्न राष्ट्रिय, क्षेत्रीय एवं अन्तर्राष्ट्रियस्तरका असल अभ्यासहरूलाई अवलम्वन गरिने।

११.४९ साइवर सुरक्षा अभिवृद्धी एवम् साइवर अपराध नियन्त्रण गर्न द्विपक्षिय एवं बहुपक्षिय समझदारी गरिने।

११.५० साइवर सुरक्षा व्यवस्थालाई समयानुकूल परिष्कृत एवं परिमार्जन गर्न अन्तर्राष्ट्रिय क्षेत्रमा अवलम्बन गरिएका असल अभ्यास एवम् नविनतम अवधारणा र प्रविधिको अवलम्बन गरिने।

११.५१ साइबर सुरक्षा सम्बन्धी अन्तर्राष्ट्रिय एवम् क्षेत्रीय संझौताहरूको कार्यान्वयन एवं आवश्यक बाध्यात्मक मापदण्डहरु लागु गरिने ।

११.५२ साइबर सुरक्षाको प्रत्याभुति गर्न तथा अन्तर्राष्ट्रिय दूरसञ्चार संघ (ITU) अनुरूप सूचना तथा सञ्चार प्रविधिको प्रयोगमा सुरक्षा र विश्वसनीयता निर्माण गर्न विश्वव्यापी साइबर सुरक्षा सूची अभ्यास (Global Cyber security Index Exercise) को सञ्चालन गरिने।

११.५३ साइवर सुरक्षा सम्बन्धी विश्वव्यापी जोखिमलाई न्यूनिकरण गर्न साइबर सुरक्षा क्षेत्रमा कार्यरत क्षेत्रीय एवं अन्तर्राष्ट्रिय संगठनहरुसंग आबद्ध भई सहकार्य गरिने।

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

११.५४ बालबालिकाका लागि अनुपयुक्त अनलाइन सेवाहरूमा पहुँच निषेधित गरिने।

११.५५ इन्टरनेट तथा सामाजिक सञ्जालको प्रयोग मार्फत हुने लैंगिक हिंसालाई न्युनिकरण गरिने।

११.५६ इन्टरनेट तथा सामाजिक सञ्जालको प्रयोग गरी झुठ्ठा खबर (Fake News) सम्प्रेषण गर्ने कार्यलाई नियमन गरिने।

११.५७ राष्ट्रिय सुरक्षामा आँच पुर्याउने, घृणा वा द्वेष फैलाउने, अनलाइन उत्पिडन (Online harassment) र साइबर बुलिङ्ग गर्ने, विभिन्न जातजाति र समुदायबिचको सुमधुर सम्बन्धमा खलल पुऱ्याउने किसिमको डिजिटल सामाग्रिको सम्प्रेषणलाई नियमन गरिने।

११.५८ स्प्याम (Spam) मेसेजहरू सम्प्रेषण गर्ने कार्यलाई नियमन गरिने।

१२. संस्थागत व्यवस्थाः

१२.१ विषयगत निकायहरूको भूमिका र जिम्मेवारी

१२.१.१ यस नीतिको कार्यान्वयनमा नेतृत्वदायी र प्राविधिक सहयोगी भूमिका सञ्चार तथा सूचना प्रविधि मन्त्रालयको रहनेछ।

१२.१.२ आफ्नो क्षेत्रमा परेका रणनीति एवं कार्यनीतिहरूको प्रभावकारी कार्यान्वयन गर्ने जिम्मेवारी विषयगत मन्त्रालयहरूको हुनेछ।

१२.२ निर्देशक समिति

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

(क) मन्त्री/राज्य मन्त्री सञ्चार तथा सूचना प्रविधि मन्त्रालय	अध्यक्ष
(ख) सचिव, प्रधानमन्त्रि तथा मन्त्रिपरिषद्को कार्यालय	सदस्य
(ग) सचिव, कानुन, न्याय तथा संसदीय मामिला मन्त्रालय	सदस्य
(घ) सचिव, गृह मन्त्रालय	सदस्य
(ङ) सचिव, अर्थ मन्त्रालय	सदस्य
(च) सचिव, रक्षा मन्त्रालय	सदस्य
(छ) सचिव, शिक्षा विज्ञान तथा प्रविधि मन्त्रालय	सदस्य
(ज) सचिव, महिला बालबालिका तथा समाज कल्याण मन्त्रालय	सदस्य
(झ) सचिव, सञ्चार तथा सूचना प्रविधि मन्त्रालय	सदस्य सचिव

१२.३ समन्वय समिति :

यस नीतिको कार्यान्वयनको लागि अन्तरनिकाय समन्वय एवं सहजिकरण गर्न देहाय बमोजिमको समन्वय समिति रहनेछः

१) सचिव, सञ्चार तथा सूचना प्रविधि मन्त्रालय	अध्यक्ष
२) सहसचिव, प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय	सदस्य
३) सहसचिव, कानुन, न्याय तथा संसदीय मामिला मन्त्रालय	सदस्य
४) सहसचिव, शिक्षा, विज्ञान तथा प्रविधि मन्त्रालय	सदस्य
५) सहसचिव, गृह मन्त्रालय	सदस्य
६) सहसचिव, अर्थ मन्त्रालय	सदस्य
७) सहसचिव, रक्षा मन्त्रालय	सदस्य
८) सहसचिव, महिला बालबालिका तथा समाज कल्याण मन्त्रालय	सदस्य
९) अध्यक्ष, कम्प्युटर एसोसिएसन अफ नेपाल महासंघ	सदस्य
१०)सहसचिव, सूचना प्रविधि महाशाखा सञ्चार तथा सूचना प्रविधि मन्त्रालय	सदस्य सचिव

समन्वय समितिको काम, कर्तव्य र अधिकार

१. यस नीतिको प्रभावकारी कार्यान्वयनको लागि आवश्यक कार्ययोजना तयार गरी निर्देशक समिति समक्ष पेश गर्ने।

२. यस नीति अन्तर्गत सञ्चालन हुने कार्यक्रम तथा क्रियाकलापहरूको प्रभावकारी कार्यान्वयनमा सहजिकरण, अनुगमन तथा मुल्यांकन गर्ने।

३. निर्देशक समितिद्वारा निर्देशन भएका अन्य कार्यहरू गर्ने।

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

(क) कार्यसमूहको संरचनाः

निम्नानुसारको संरचनामा राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह (National Cyber Security Strategy Working Group – NCSWG) को गठन गरी क्रियाशील बनाइनेछ। यसरी कार्य समूह गठन गर्दा सुरक्षाको दृष्टिकोणबाट विशिष्टीकृत सामग्रीहरू पर्याप्त सुरक्षा जानकारी भएका सदस्यहरूमा मात्र सीमित 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) वरिष्ठ निर्देशक, नेपाल दूरसञ्चार प्राधिकरण सदस्य

६) उपसचिव (सूचना प्रविधि), प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय सदस्य

७) मन्त्रालयले मनोनित गरेको एक जना महिला सहित २ जना निजी क्षेत्रको प्रतिनिधि सदस्य

८) उपसचिव, साइबर सुरक्षा शाखा सञ्चार तथा सूचना प्रविधि मन्त्रालय सदस्य सचिव

(ख) कार्य समूहको काम र कर्तव्य देहाय बमोजिम हुनेछ :

१) साइबर सुरक्षा ऐन मस्यौदा गर्ने।

२) साइबर सुरक्षासम्बन्धी अनुसन्धान तथा विकास क्रियाकलापको समन्वय एवं प्राथमिकीकरण गर्ने।

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

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

५) साइबर सुरक्षा विपद् तथा घटनाहरूको व्यवस्थापन गर्ने ।

६) साइबर आक्रमणको सम्भावित विध्वंशकारी प्रभाव (Devastating effect) लाई ध्यानमा राखी चाल्नुपर्ने कदमहरु निर्धारण गर्ने।

७) साइबर सुरक्षाका लागि प्राविधिक मापदण्ड मस्यौदा गर्ने।

८) जोखिम आंकलन एवं आपतकालीन योजनाहरू तथा सम्भाव्य जोखिम न्यूनीकरणका उपायहरू पहिचान गर्ने।

१२.५ राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह (NITERT) :

सरकार, सरकारी संस्थाहरू, कानून कार्यान्वयन गर्ने निकायहरू, व्यवसायहरू एवं जनतालाई साइबर सुरक्षासँग सम्बन्धित सेवाहरू प्रदान गर्ने जिम्मेवारी राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह हुनेछ।

समुहको काम, कर्तव्य

- मानवीय तथा प्राकृतिक कारणले हानी नोक्सानी पुगी राष्ट्रिय सुरक्षा, अर्थव्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य वा सार्वजनिक

सुरक्षासँग सम्बन्धित सूचना प्रविधि प्रणाली सञ्चालन बन्द भएमा यथाशीघ्र सो प्रणालीलाई पुनः सञ्चालनमा ल्याउन सहायता गर्ने।

- नेपालभित्र साइबर सुरक्षाको अवस्थाको निरन्तर अनुगमन गर्ने।
- अन्तर्राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समुहहरूको विभिन्न छाता संगठनहरूमा आवद्ध भइ साइबर सुरक्षाको क्षेत्रमा राष्ट्रिय सम्पर्क विन्दुको रुपमा काम गर्ने।
- साइबर सुरक्षा सम्बन्धी घटनाको विस्तृत अध्ययन तथा विश्लेषण गरी सम्बन्धित निकाय वा व्यक्तिलाई जानकारी गराउने तथा सोको समाधानको लागि सहजिकरण गर्ने।
- साइबर सुरक्षा प्रवर्धन गर्ने, जनचेतना अभिवृद्धि गर्ने, २४/७ सम्पर्क विन्दुको रुपमा काम गर्ने, डिजिटल फोरेन्सिक अनुसन्धान गर्ने, साइबर सुरक्षा सम्बन्धी उत्तम अभ्यास, मापदण्ड एवं निर्देशिका अनुरूप मूल्याङ्कन र प्रमाणीकरणका लागि आवश्यक पूर्वाधार व्यवस्थापन गर्ने।
- साइबर अपराध एवं साइबर सुरक्षा घटनाबाट नागरिकहरू, व्यवसायहरू तथा सरकार कहाँसम्म प्रभावित भएका छन् भनी विश्लेषण गर्न समन्वयात्मक सर्भेक्षण तथा आंकलन गर्ने।
- राष्ट्रिय र क्षेत्रीय स्तरमा साइबर सुरक्षासम्बन्धी तयारी (Cyber Security Readiness) को स्तर मापन गर्ने ।
- आवश्यकता अनुसार क्षेत्रगत सहायता समुहहरूलाई निर्देशन दिने तथा सहजिकरण गर्ने।
- प्राविधिक तथा संस्थागत सुरक्षाका उपायहरू विकास एवं कार्यान्वयन गर्नुका साथै अत्यावश्यक सरकारी सेवाहरूलाई सुरक्षित गर्न योजना तर्जुमा गर्ने।

१२.६ महिला तथा बालबालिका अनलाइन सुरक्षा कार्यसमूह (Female and Child Online Protection Working Group - COPWG) को गठन गरिनेछ ।

- कार्यसमुहको गठन महिला तथा बालबालिका हेर्ने मन्त्रालय अन्तर्गत हुनेछ।
- 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।
- कार्यसमूहले महिला तथा बालबालिकाको अनलाइन सुरक्षा गर्न सेवा प्रदायकहरूले अपनाउनुपर्ने विभिन्न प्राविधिक उपायहरूको निर्धारण गर्नेछ।

- कार्यसमूहले सरोकारवाला निकायसँगको सहकार्यमा महिला तथा बालबालिकाको अनलाइन सुरक्षासम्बन्धी निर्देशिका तयार गरी कार्यान्वयन गर्नेछ।

१३. आर्थिक पक्ष

१३.१ साइवर सुरक्षा नीतिको लक्ष्य प्राप्तिको लागी सरकारी, गैर सरकारी, निजी एवं अन्तराष्ट्रिय स्रोत तथा साधनको परिचालन गरिने,

१३.२ यो नीति कार्यान्वयनका लागि एक वर्षभित्र कार्यान्वयन कार्ययोजना बनाइने।

१४. कानूनी व्यवस्था

साईबर सुरक्षाका लागि आवश्यक व्यवस्थाहरुलाई नियमित गर्न तथा साईबर अपराध रोकथाम गरी सभ्य समाज निर्माणका लागि विद्यमान नियामक एवं कानूनी संरचनाहरु एक वर्षभित्र पुनरावलोकन गरिनेछ। साइवर सुरक्षा ऐन तथा अन्य आवश्यक कानूनहरुको निर्माण गरिनेछ। विद्यमान विद्युतीय कारोवार ऐनलाई अन्तर्राष्ट्रिय मापदण्ड अनुरुप परिमार्जन गरिनेछ।

१५. अनुगमन र मूल्यांकन

यस नीतिको वार्षिकरुपमा समीक्षा गरी प्रत्येक पाँच वर्षमा पुनरावलोकन गरिनेछ। नीति कार्यान्वयनको अनुगमन तथा मूल्याङ्कन सञ्चार तथा सूचना प्रविधि मन्त्रालयले गर्नेछ।

१६. जोखिम

- संवेदनशील पूर्वाधार प्रदायकहरूले प्रदान गर्ने सेवाहरूको सुरक्षा पहुँच गर्न कठिनाई हुन सक्ने ।
- नीजि क्षेत्रको सहभागिता तथा योगदानमा निरन्तरता प्राप्त गर्न कठिनाई हुन सक्ने,
- आवश्यक आर्थिक श्रोतको उपलब्धतामा कठिनाई हुन सक्ने,
- राजनैतिक एवं प्रशासनिक समन्वयात्मक वातावरण निर्माणमा कठिनाई हुन सक्ने।
- साइबर सुरक्षा सम्बन्धी दक्ष जनशक्ति व्यवस्थापनमा कठिनाई हुनसक्ने।
-