राष्ट्रिय साइबर सुरक्षा नीति
२०७३ (२०१६)

विषय सूची

१. पृष्ठभूमि १

२. मुख्य मुद्दा/विषय तथा चुनौतीहरू ३

३. राष्ट्रिय परिकल्पना ४

४. निर्देशक सिद्धान्तहरू ४

५. साइबर सुरक्षा नीतिका लक्ष्यहरू ५

६. राष्ट्रिय साइबर सुरक्षा निर्देशिकाको विकास ६

७. आवश्यक संगठनात्मक संरचनाहरूको सशक्तीकरण ७

८. बाल अनलाइन सुरक्षा १४

९. संवेदनशील पूर्वाधारको सुरक्षा १५

१०. नीतिगत ढाँचाको कार्यान्वयन २१

११. राष्ट्रिय सूचना तथा सञ्चार प्रविधि गुरुयोजना/राष्ट्रिय विद्युतीय रणनीतिको स्थापना २२

१२. स्रोत परिचालन २२

१३. कानुनी प्रबन्धहरू २२

१४. अनुगमन तथा मूल्याङ्कन २२

१. पृष्ठभूमि

१.१ नेपाल सरकारले सूचना तथा सञ्चार प्रविधिको विकाससँग सम्बन्धित हुँदै सन् २०१५ मा **राष्ट्रिय सूचना तथा प्रविधि नीतिमार्फत** मुख्य प्राथमिकताहरूको (key priorities) परिभाषा गरेको छ। यसले ब्रोडब्याण्ड पहुँचको वृद्धि (increase of broadband access) एवं विद्युतीय व्यापार (e-Commerce) क्षेत्रलाई सशक्तीकरण तथा प्रोत्साहित गर्ने उपायहरूलाई (measures) समाहित गरेको छ। यसै नीतिमा आधारित भई सूचना तथा सञ्चार प्रविधिले स्वास्थ्यदेखि शिक्षा लगायतका विभिन्न क्षेत्रहरूमा बढ्दो भूमिका निर्वाह गर्नेछ।

१.२ **राष्ट्रिय सूचना तथा सञ्चार प्रविधि नीति** (National Information and Technology Policy -ICT Policy) ले विश्वास तथा सुरक्षाको वातावरण निर्माणको महत्त्वमा जोड (highlight) दिन्छ। यसले नागरिकहरूको मौलिक हकको संरक्षणका साथै अपराध अनुसन्धानमा समेत क्षमता विकास गर्न बल पुऱ्याउनेछ।

१.३ सूचना तथा सञ्चार प्रविधिले नेपालमा व्यवसायी, जनता तथा सरकारलाई विना कुनै संशय अनुपम अवसरहरू (unique opportunities) प्रदान गर्दछ। अन्य देशहरूको तथ्याङ्कीकरणसँगको अनुभवले (experience with digitalization) सूचना तथा सञ्चार प्रविधिको प्रयोगबाट अर्थतन्त्रलाई उत्प्रेरित (stimulate) गर्ने तथा सेवा क्षेत्रलाई सशक्तीकरण गर्ने संभाव्यता दर्शाउँछ। यसले ज्ञानमा पहुँच पुऱ्याउन सहज बनाउनुका साथै शिक्षामा (विकसित भागहरूमा मात्र नभई विशेषतः ग्रामीण क्षेत्रहरूमा) समेत महत्त्वपूर्ण भूमिका निर्वाह गर्दछ। राष्ट्रिय संवेदनशील पूर्वाधारहरू (national critical infrastructures) जस्तै विद्युत् आपूर्ति एवं सरकारी सेवाहरूको कार्यक्षमता वा कार्यकुशलता र विश्वसनीयतामा सुधार गर्न यसले स्वाभाविक रूपमा सहयोग गर्दछ। तर, सोही समयमा सूचना तथा सञ्चार प्रविधिको एकीकरणसँगै जोखिमको वृद्धि हुने संभावना भएकोले यसमा जोखिम आकलन (risk assessment), जोखिम व्यवस्थापन (risk management) र प्रत्युपाय (counter measure) को आवश्यकता पर्ने हुन्छ। यद्यपि सञ्जालको आवद्धता (connectivity) मा हुने वृद्धिले सेवा क्षेत्रमा विकास भए पनि साइबर आक्रमणसँग (cyber attacks) व्यवसायी तथा निजी प्रयोगकर्ता दुवैलाई क्षति पुऱ्याउने क्षमता हुन्छ। ज्ञानमा पहुँच (access to knowledge) बाट विद्यार्थी वर्गलाई फाइदा पुग्ने भए तापनि सोही प्रविधिले गैरकानुनी एवं हानिकारक विषयवस्तु (harmful content) मा पनि पहुँच पुऱ्याउने हुँदा यसतर्फ समेत सावधान हुन आवश्यक छ। सूचना तथा सञ्चार प्रविधिले संवेदनशील पूर्वाधारको सञ्चालनमा सहयोग पुऱ्याउने भए तापनि भविष्यमा यस्ता अत्यावश्यक सेवाहरूमा यिनलाई जोड्ने सञ्जालहरू (connecting networks) मार्फत टाढाबाट (remotely) आक्रमण हुन सक्ने सम्भावना हुन्छ।

१.४ संयुक्त राष्ट्र संघ तथा विश्वभरका र यस क्षेत्रका अन्य देशहरूले जस्तै जोखिम (threats) भन्दा सूचना तथा सञ्चार प्रविधिको क्षमता बढी महत्त्वपूर्ण हुन्छ भन्ने तथ्यमा सरकार पनि दृढ विश्वास राख्दछ। सञ्चार प्रविधिको प्रयोगलाई अझ सशक्तीकरण गर्दै सूचना तथा सञ्चार प्रविधि (ICT) सम्बन्धमा जारी क्रियाकलापहरूलाई समर्थन गर्नका लागि **राष्ट्रिय सूचना तथा सञ्चार प्रविधि नीति** का अतिरिक्त **राष्ट्रिय साइबर सुरक्षा नीति**लाई पनि अपनाउने (adopt) निर्णय भएको छ। यो नीति मौजुदा नीतिहरूमा आधारित भई निर्माण भएको र सूचना तथा सञ्चार प्रविधिको प्रयोगमा बचाव र सुरक्षा (safety and security) को वृद्धि गर्न यसले लक्ष्य तथा उद्देश्यहरू (goals and objectives) को तर्जुमा गरेको छ। यस नीतिले **राष्ट्रिय सूचना तथा सञ्चार प्रविधि नीति**मा समाविष्ट विशेषतः सूचना तथा सञ्चार प्रविधिमा सुरक्षा तथा विश्वास अभिवृद्धि गर्ने कुरासँग सम्बन्धित विषयको बुँदा नं. ७.२.१ लाई विशेष ध्यान दिएको छ। अन्य कुराका अतिरिक्त यसले शहस्राब्दी विकास लक्ष्य (Millennium Development Goals) का उद्देश्यहरू, अन्तर्राष्ट्रिय दूरसञ्चार संघ साधिकार सम्मेलन–बुसान, २०१४ (Final Acts of the ITU Plenipotentiary Conference, Busan, 2014) तथा अन्तर्राष्ट्रिय दूरसञ्चार संघ विश्वव्यापी साइबर सुरक्षा एजेन्डा (ITU Global Cyber security Agenda) बाट पारित सिफारिसहरूलाई (Recommendations) प्रतिविम्बित गरेको छ।

१.५ प्रस्तुत नीति अन्तर्राष्ट्रिय दूरसञ्चार संघ (ITU) को प्राविधिक सहयोगमा नेपाल दूरसञ्चार प्राधिकरणबाट तयार गरिएको हो। सरकारी, गैरसरकारी तथा सरोकारवालाहरूको (stakeholders) परामर्शसहित राष्ट्रिय, क्षेत्रीय एवं अन्तर्राष्ट्रिय विज्ञहरूसँग विचारविमर्श गरी यो नीति निर्माण गरिएको हो। यस नीतिको मस्यौदा तयार गर्ने क्रममा विभिन्न खालका प्रश्नावलीका आधारमा सूचना तथा सञ्चार प्रविधि (ICT) को प्रयोगमा देशको परिस्थिति र सार्वजनिक तथा निजी क्षेत्रका अपेक्षाहरूलाई आकलन गरिएको थियो।

२. मुख्य मुद्दा/विषय तथा चुनौतीहरू

२.१ साइबरसम्बन्धी आशंका/डरहरू (threats) द्रुत गतिमा विकसित भइरहेका छन्। नेपालका जनता र व्यवसायको यस्ता आशंका/डरहरू सम्बन्धी अद्यावधिक सूचनामा पहुँचका साथै तिनीहरूको प्रतिरक्षा गर्ने विषयलाई सुनिश्चित गर्नु नितान्त आवश्यक छ। यसको सुनिश्चितताबाट चुनौतीलाई सम्बोधन गर्न संस्थागत क्षमताको निर्माणका साथ आशंका/डर सम्बन्धी अनुगमन गरी सम्बन्धित सूचना तथा सेवाहरू उपलब्ध हुनेछन्।

२.२ आजभोलि साइबर आक्रमणहरू धेरै हदसम्म अन्तर्राष्ट्रिय प्रकृतिका भएका छन् र अपराधीहरूले अति विज्ञता र सावधानीका (sophistication) साथ आफ्नो कार्य गर्दछन्। यी आशंका/डरहरूसँग प्रभावकारी रूपमा सामना गर्नमा अन्तर्राष्ट्रिय सहयोगको आवश्यकता हुन्छ। संस्थागत क्षमता (institutional capacities) का साथै नीति तथा

कानुनी ढाँचालाई (legal framework) अन्तर्राष्ट्रिय उत्तम अभ्यास (international best practices) अनुरूप विकास गरी नेपालले चुनौतीहरूलाई सम्बोधन गर्नेछ।

२.३ जोखिम परिदृष्य (risk landscape) मा भएका प्रगतिको निरन्तर अनुगमन गर्न, जनता, व्यवसायीहरू तथा सरकारका लागि सेवाहरू प्रदान गर्न, आक्रमणहरूको रोकथाम गर्नका साथै रोकथाम गर्न नसकिने प्रकृतिका आक्रमणको छानबिन गर्नका लागि शसक्त संस्थागत क्षमताको आवश्यकता पर्दछ। विद्यमान क्षमतालाई सशक्तीकरण गर्नाका साथ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (National Computer Emergency Response Team (CERT) - Nep CERT) को गठन र कार्यान्वयनबाट नयाँ क्षमताको विकास गरी नेपालले चुनौतीहरूलाई सम्बोधन गर्नेछ।

२.४ संसारभर कुनै पनि सरकार एक्लै सबै सम्भाव्य साइबर जोखिमबाट जनता र व्यवसायलाई सुरक्षा प्रदान गर्न सक्षम हुँदैन। नेपालले यी चुनौतीहरू निम्नलिखित उपायहरू अवलम्बन गरी सम्बोधन गर्नेछः

- सरकारी कार्यको प्राथमिकता क्षेत्रहरू (focus area) को स्पष्ट परिभाषाका साथ सशक्त निजी सार्वजनिक साझेदारीसँग संयोजन गरी;
- व्यवसायीहरूका साथै जनतालाई निरोधात्मक उपायहरू (preventive measures) अवलम्बन गर्न अभिप्रेरित र सशक्तीकरण गरी।

२.५ आक्रमणहरूको रोकथाम (prevention) र गैरकानुनी कार्यहरूको पहिचान (detection) का साथै तिनको प्रतिस्थापन (recovery) का लागि दक्ष विज्ञहरूको आवश्यकता पर्दछ। वर्तमान समयमा यस्ता विज्ञहरूको नेपालमा कमी छ। देशभित्रै यस्तो विज्ञता सृजना गर्ने वातावरण तयार गरी नेपालले चुनौतीहरूलाई सम्बोधन गर्नेछ।

२.६ सामान्यतः सरकार एवं विशिष्टीकृत प्रतिष्ठानहरूलाई सुरक्षासम्बन्धी प्रचलन (trends) तथा नयाँ उपलब्धिको जानकारी दिनका लागि देशमा भएका आक्रमणहरूका (attacks) बारेमा अद्यावधिक सूचनाको आवश्यकता पर्दछ। नेपालले चुनौतीहरूलाई उपयुक्त उपायहरूको (mechanism) विकास गरी सम्बोधन गर्नेछ। यस सम्बन्धमा द्विदिशात्मक सूचना आदानप्रदानलाई (bi-directional exchange) समर्थन गर्न सरकार कटिबद्ध रहनेछ ।

३. राष्ट्रिय परिकल्पना

जोखिम/आशंकाहरूलाई बुझी एवं सम्बोधन गर्दै नेपालका जनता, व्यवसायीहरू एवं सरकारले भरपर्दो, सुरक्षित तथा लचिलो साइबर स्पेश (resilient cyber space) को पूरा सुविधा उपयोग गर्न, तिनीहरूलाई सूचना बाँड्न तथा ज्ञानको पहुँचमा सक्षम बनाउन, अपराधीहरूलाई सुविधा घटाउन, स्थिर आर्थिक तथा सामाजिक विकास सुनिश्चित गर्न र आधारभूत प्रजातान्त्रिक संरचनाहरूलाई सुरक्षित गर्न **राष्ट्रिय साइबर सुरक्षा नीति**को परिकल्पना गरिएको छ।

४. निर्देशक सिद्धान्तहरू

४.१ उपयुक्त राष्ट्रिय परिकल्पना सहित, **राष्ट्रिय सूचना सञ्चार प्रविधि नीति** (National ICT Policy) द्वारा विकसित एवं परिभाषित लक्ष्य प्राप्त गर्न सरकारले जनता, व्यवसायीहरू एवं सरकारी संस्थाहरूको संरक्षणका लागि आवश्यक सुरक्षित ढाँचा प्रदान गर्ने लक्ष्य लिनेछ।

४.२ यस नीतिको कार्यान्वयन अन्य कुराहरूका अतिरिक्त राष्ट्रिय परिकल्पनाद्वारा निर्देशित हुनेछ। यसको कार्यान्वयन सरकारी नेतृत्वमा निजी क्षेत्रद्वारा सञ्चालित (government led and private sector driven) हुनेछ। यसको कार्यान्वयनका लागि आधारहरूमध्ये सार्वजनिक निजी साझेदारी [public–private partnership- (PPP)] एक बन्नेछ।

४.३ **सूचना तथा सञ्चार प्रविधि नीति** (ICT Policy) मा वर्णित उपायहरूको अवलम्बनबाट देशभरको आवद्धता (connectivity) मा ठुलो प्रभाव पर्नेछ भन्नेमा सरकार सचेत छ। यसका अतिरिक्त ब्याण्डविथमा वृद्धि (increase in bandwidth) सँगै नयाँ सेवाहरू उपलब्ध हुने र तीमध्ये केही सुरक्षा चासो (security concerns) पनि सँगसँगै रहनेछ। परिणामस्वरूप सेवा तथा आवद्धता (services and connectivity) मा भएको बढोत्तरीको साथसाथै साइबर सुरक्षाका उपायहरू कार्यान्वयन भएको सुनिश्चित गर्न सरकारले यस नीतिको समयबद्ध कार्यान्वयनलाई प्राथमिकता दिनेछ।

४.४ यो नीति लागू गर्न उपयुक्त कानून बनाई नियमनको व्यवस्था गरिनेछ। यस्तो कानून विशेषतः (legislation), साइबर अपराध (cyber crime) एवं सूचना तथा सञ्चार प्रविधिको आपराधिक दुरुपयोग विरुद्ध केन्द्रित हुनेछ। नियमन (regulation), साइबर सुरक्षा (cyber security) को सम्बन्धमा न्यूनतम प्राविधिक मापदण्ड (technical minimum standard) निर्धारणमा समेत विशेष रूपमा केन्द्रित हुनेछ।

४.५ संयुक्त राष्ट्र संघीय महासभाका प्रस्तावहरू (UNGA Resolutions) का साथै अन्तर्राष्ट्रिय दूरसञ्चार संघबाट लागू हुने सुझाउहरू (International Telecommunication Union – ITU Recommendations) मा आधारित भई सूचना तथा सञ्चार प्रविधि (ICT) मा सुरक्षा तथा विश्वासको सृजना गर्न राष्ट्रिय, क्षेत्रीय एवं विश्वस्तरका सान्दर्भिक (relevant) उत्तम अभ्यासहरू (best practices) लाई यस नीतिको कार्यान्वयनले मनन गर्नेछ।

५. साइबर सुरक्षा नीतिका लक्ष्यहरू

५.१ नेपालले प्राविधिक निर्देशिका (technical guidelines) एवं राष्ट्रिय साइबर सुरक्षा रणनीतिको अन्य प्राविधिक तथा संगठनात्मक अंगहरूको विकास गर्नेछ। राष्ट्रिय मागका अतिरिक्त अन्तर्राष्ट्रिय उत्तम अभ्यासहरू (International Best Practices) लाई ध्यानमा

राखी यो निर्देशिका रणनीति साइबर सुरक्षा कार्य समूह (dedicated Cyber security Working Group) द्वारा तयार गरिनेछ।

५.२ यस क्षेत्रका साथै नेपालमा विद्यमान संरचनाहरूको प्रयोगलाई केन्द्रित गर्दै आवश्यक संगठनात्मक संरचनाहरूलाई सशक्त गरिनेछ जसले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (Nep CERT) को स्थापनालाई समेट्नेछ।

५.३ नेपाल सरकार, नागरिक, व्यवसायका आधारभूत सेवाहरू तथा साइबर सुरक्षासँग सम्बन्धित (Actionable Intelligence) विषयमा पहुँच हुनेछ।

५.४ साइबर सुरक्षाका बारेमा ज्ञानको स्तर तथा नेपाली नागरिक र व्यवसायलाई साइबर जोखिमका विरुद्ध सुरक्षाका उपायहरूलाई उच्च तहमा पुऱ्याई सरकार, व्यवसायहरू र नागरिकका लागि विज्ञताका साथै आधारभूत साधन (basic tools) र सेवाहरू उपलब्ध गराइनेछ।

५.५ सरोकारवालाहरू बिच सूचनाको निरन्तर आदानप्रदान गर्न दिने वातावरणको सृजना गरिनेछ।

५.६ अपराधीकरण, अनुसन्धान, विद्युत्तीय प्रमाण तथा अन्तर्राष्ट्रिय सहयोगका (criminalization, investigation, electronic evidence and international cooperation) साथै मौलिक अधिकारहरूको संरक्षण (protection of fundamental rights) का सन्दर्भमा उच्चतम क्षेत्रीय एवं अन्तर्राष्ट्रिय मापदण्ड/स्तर कायम गर्न नेपालको कानुनी तथा नीतिगत व्यवस्थालाई सशक्त बनाइनेछ।

५.७ साइबर सुरक्षासम्बन्धी विश्वव्यापी जोखिमलाई मध्यनजर गरी त्यस्ता जोखिमहरूका विरुद्ध अन्तर्राष्ट्रिय सहयोगमा सहभागी हुने दिशमा नेपाललाई सक्षम बनाइनेछ।

५.८ खास साइबर जोखिमहरूको न्युनीकरण एवं प्राविधिक सुरक्षा उपायहरूको कार्यान्वयन गरी बालबालिकाका लागि सुरक्षित वातावरण सृजना गरिनेछ।

५.९ संवेदनशील आधारभूत पूर्वाधारसँग सम्बन्धित साइबर जोखिमहरूको सुरक्षालाई सबलीकरण गरिनेछ।

५.१० समुन्नत भविष्यको आधार बनाउँदै, नयाँ बजारहरूको विकास र विविधीकरण गर्न यस नीतिले व्यवसायहरूलाई सहयोग पुऱ्याउनेछ ।

५.११ नेपालको साइबर सुरक्षा नीतिले नेपाली नागरिहरूको गोपनीयताको हक एवं मौलिक स्वतन्त्रताको संरक्षण गर्नाका साथै व्यक्तिगत एवं सामूहिक सुरक्षाका उपायका बिच सन्तुलन कायम गर्नेछ ।

६. राष्ट्रिय साइबर सुरक्षा निर्देशिकाको विकास

६.१ निम्नानुसारको संरचनामा राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह (National Cyber Security Strategy Working Group – NCSWG) को स्थापना गरिनेछ :-

सचिव, सूचना तथा सञ्चार मन्त्रालय	अध्यक्ष
कानून कार्यान्वयन निकाय	सदस्य
सचिव, विज्ञान तथा प्रविधि मन्त्रालय	सदस्य
सचिव, गृह मन्त्रालय	सदस्य
अध्यक्ष, नेपाल दूरसञ्चार प्राधिकरण	सदस्य
प्रतिनिधि, निजी क्षेत्र	सदस्य
प्रतिनिधि, डोमेन विशेषज्ञ (domain expert)	सदस्य
प्रतिनिधि, नागरिक समाज	सदस्य

सुरक्षाको दृष्टिकोणबाट विशिष्टीकृत सामग्रीहरू पर्याप्त सुरक्षा जानकारी (Adequate security clearance) भएका सदस्यहरूमा मात्र सीमित गरिनेछ।

६.२ राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह (NCSWG) ले विशेष साइबर सुरक्षा निर्देशिका तयार गर्नेछ । यो निर्देशिका नीतिगत विवरणहरू (policy statements) भन्दा माथि उठी ठोस उपायहरूमा केन्द्रित हुनेछ। यसले निम्नलिखित विषयहरूलाई सम्बोधन गर्नेछः

- सरकारी र निजी क्षेत्रको जिम्मेवारी,
- विधिहरूको परिभाषा,
- प्राविधिक विवरणहरू र
- जोखिम निर्धारण (risk assessment) एवं आपतकालीन योजनाहरू (emergency plans) ।

जिम्मेवारीका सम्बन्धमा विभिन्न निकायहरूको भूमिका तथा उत्तरदायित्वहरू स्पष्ट रूपमा उल्लेख गरिनेछ।यसमा प्राविधिकका साथै व्यवस्थापकीय जिम्मेवारी समावेश हुन सक्दछ। विपद् तथा घटनाहरूको पर्याप्त व्यवस्थापन कुनै पनि साइबर प्रतिरक्षा रणनीति (cyber defense strategy) को मुख्य अंश (key component) हो भन्नेमा सरकारले विशेष ध्यान दिनेछ।साइबर आक्रमणको (cyber attack) सम्भावित विध्वंशकारी प्रभाव (devastating effect) लाई ध्यानमा राखी विभिन्न परिस्थितिमा निश्चित व्यक्ति तथा संस्थाले चाल्नुपर्ने कार्यहरू सम्बन्धी स्पष्ट नियम एवं कार्यविधिहरूको आवश्यकता हुन्छ।यी कार्यविधिहरूले साइबर सुरक्षा सम्बन्धमा सरकारी प्रक्रियाबारे उल्लेख गर्नेछन्। यसमा नयाँ कर्मचारीलाई दिइने अनिवार्य तालिम विधिहरू लगायत विदेश भ्रमणका वेलामा अपनाउनु पर्ने ठोस सुरक्षा प्रक्रियासम्म हुन सक्नेछ।प्रक्रियाहरूमा

विशेष गरी रोकथाम, तयारी, पहिचान, प्रतिक्रिया तथा पुनर्लाभ (prevention, preparedness, detection, response and recovery) सम्बन्धमा उल्लेख हुनेछ। यस अतिरिक्त प्रस्तुत खण्डमा अनुसन्धान तथा विकास योजनाहरू (research and development plans) लाई सम्बोधन गरिनुपर्दछ। साइबर सुरक्षाका लागि सरकारी तथा उद्योगव्यापी (industry wide) प्राविधिक मापदण्ड (technical specification), जस्तै गोप्य दस्तावेजको लागि आवश्यक न्यूनतम कुटलेखन (encryption) सम्बन्धी मापदण्डहरू तय गर्दा विभिन्न मापदण्डका कारणबाट द्विविधा नहोस् भन्नेमा ध्यान दिनुपर्नेछ। जोखिम आकलन एवं आपतकालीन योजनाहरू (risk assessment and emergency plans) ले अति सम्भाव्य जोखिमहरू न्यूनीकरण गर्ने बारेमा पनि उल्लेख गर्नुपर्नेछ।

६.३ निर्देशिका तयार गर्दा नयाँ हुने विकास (प्राविधिक परिमार्जन र जोखिमको मात्रा) लाई समायोजन (adjustment) गर्न मिल्ने किसिमले तयार गर्नुपर्नेछ। यसका अतिरिक्त निर्देशिकाले निजी क्षेत्रसँगको सम्बन्ध तथा अन्तरनिर्भरताको स्पष्ट संकेत गर्नुपर्नेछ।

६.४ साइबर सुरक्षासम्बन्धी अनुसन्धान तथा विकास क्रियाकलापको समन्वय र प्राथमिकीकरण (coordination and prioritization) को जिम्मेवार राष्ट्रिय साइबर सुरक्षा रणनीतिक कार्यसमूह (NCSWG) हुनेछ। साथै, यसले स्थानीय साइबर सुरक्षा समुदायको निर्माण र सशक्तीकरण समेतमा ध्यान दिनेछ। यसबाहेक यसले सूचना सुरक्षा पेशाकर्मीहरू (Information Security professionals) का लागि आवश्यक न्यूनतम योग्यताको पहिचान गर्नेछ।

७. आवश्यक संगठनात्मक संरचनाहरूको सशक्तीकरण

७.१ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (**Nep CERT**) को स्थापना

७.१.१ नेपालमा एउटा स्वतन्त्र राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (Nep CERT) को स्थापना गरिनेछ। सूचना तथा सञ्चार मन्त्रालय/विज्ञान तथा प्रविधि मन्त्रालय/नेपाल दूरसञ्चार प्राधिकरणले यसको सुपरिवेक्षण एवं अनुगमन गर्नेछ। सरकार, सरकारी संस्थाहरू, कानून कार्यान्वयन गर्ने निकायहरू, व्यवसायहरू एवं जनतालाई साइबर सुरक्षासँग सम्बन्धित सेवाहरू प्रदान गर्ने जिम्मेवारी राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (**Nep CERT**) को हुनेछ। यसले आफ्नो ध्यान साइबर सुरक्षा प्रवर्धन गर्न, जनचेतना अधिवृद्धि गर्न, अनुरोध गरिए अनुसार संस्थाहरू तथा व्यवसायहरूलाई साइबर आक्रमणको रोकथाम, पहिचान र पहल गर्न, २४/७ सम्पर्क विन्दु कायम गर्न, डिजिटल फोरेन्सिक अनुसन्धान (digital forensic investigation) गर्न, घटना बारेमा प्रतिवेदनहरू प्राप्त तथा वितरण गर्न, संवेदनशील आधारभूत संरचना (critical infrastructure provider) हरूलाई विशेष सहायता प्रदान गर्नमा केन्द्रित गर्नेछ।

राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले साइबर सुरक्षासम्बन्धी उत्तम अभ्यास, मापदण्ड एवं निर्देशिका (जस्तै ISO 27001) अनुरूप एकरूपता मूल्याङ्कन (conformity assessment) र प्रमाणीकरणका लागि आवश्यक पूर्वाधार सृजना गर्नुपर्नेछ।

७.१.२ राष्ट्रिय सूचना तथा सञ्चार प्रविधि नीति कार्यान्वयन संचालन समितिको कार्यदेश संशोधन गरिनेछ। यस नीतिको कार्यान्वयनको सन्दर्भमा यसले प्राथमिकता क्षेत्रको परिभाषा गर्नाका साथै पथप्रदर्शन गर्नेछ।

७.१.३ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले साइबर अपराध विरुद्ध कार्यरत एवं साइबर सुरक्षाका क्षेत्रमा क्रियाशील सबै विद्यमान सरकारी एवं गैरसरकारी संस्थाहरूको पहिचान गर्नेछ। साथै यसले विभिन्न संस्थाहरूको कार्यदेश (mandate), स्रोत र अनुभवका बारेमा प्रतिवेदनको मस्यौदा गर्नेछ, जसमा सहकार्य (synergy), पारस्परिक अतिक्रमण (overlapping) तथा कमीहरूका बारेमा विश्लेषण गर्नेछ ।

७.१.४ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले काठमाडौं बाहिरका स्थानीय सम्पर्क विन्दुहरूको पहिचान गर्नेछ जसले हाल भइरहेको प्रगतिको संकलनका साथै समुदायलाई सूचना सम्प्रेषणमा सहयोग पुऱ्याउनेछ। यस प्रक्रियामा सार्वजनिक निजी साझेदारीको अवधारणालाई ध्यानमा राखिनेछ।

७.१.५ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले साइबर अपराध एवं साइबर सुरक्षा घटनाबाट नागरिकहरू, व्यवसायहरू तथा सरकार कहाँसम्म प्रभावित भएका छन् भनी विश्लेषण गर्न समन्वयात्मक सर्भेक्षण तथा आकलन (coordinated survey and assessment) गर्नेछ ।

७.२ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीद्वारा पुऱ्याइने सेवाहरू

७.२.१ यदि माग भएमा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सरकार, सरकारी संस्थाहरू, कानून कार्यान्वयन गर्ने निकायहरू, व्यवसायहरू एवं सर्वसाधारण जनतालाई साइबर सुरक्षाका बारेमा सूचना प्रदान गर्नेछ। प्राप्त अनुरोधलाई व्यवस्थित गर्न, साइबर सुरक्षा र यसको परिपालना (cyber security and compliance) मा विश्वव्यापी उत्तम अभ्यासहरूको अवलम्बन (adoption of global best practices) गर्नमा बढावा दिन, व्यावहारिक सूचना र तालिम सामग्री उपलब्ध गराउनाका साथै सार्वजनिक रूपमा उपलब्ध साधनहरूका बारेमा जानकारी दिनसक्ने गरी यसले स्रोतहरूको व्यवस्था गर्नुपर्नेछ। यसका अतिरिक्त यसले संवेदनशील पूर्वाधार प्रदायक तथा कानून कार्यान्वयन गर्ने निकायहरूका लागि परामर्शदायी सहयोग पुऱ्याउनु पर्दछ।

७.२.२. राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सम्भव भएसम्म देशमा विद्यमान मुनाफारहित ढङ्गले गैरव्यावसायिक स्तरमा सेवा, सामग्री तथा सूचना प्रदान गरिरहेका संस्थाहरूसँग सहकार्य गर्नेछ र नयाँ सामग्रीको विकास गर्नुको सट्टा विद्यमान सामग्रीको प्रयोग बारेमा खोजी गरी मूल्याङ्कन गर्नेछ।

७.२.३. यदि माग भएमा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सरकार, सरकारी संस्थाहरू, कानून कार्यान्वयन गर्ने निकायहरू एवं व्यवसायीहरूलाई सूचना सुरक्षासम्बन्धी योजना तर्जुमा र व्यवस्थापन गर्न सहयोग गर्नेछ।

७.२.४ साइबर सुरक्षासम्बन्धी घटनाहरू (incidents) सँगको संघर्षमा आकस्मिक तयारीको स्तर लेखाजोखा गर्न राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले राष्ट्रिय, क्षेत्रीय र प्रवेश स्तरमा (entry level) साइबर सुरक्षासम्बन्धी गृहकार्य (drills) नियमित रूपमा सञ्चालन गर्नेछ।

७.३. सुरक्षित साइबर परिवेशको सृजना – राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली

७.३.१ व्यवसायहरू तथा जनतालाई साइबर सुरक्षासँग सम्बन्धित जोखिमहरूबाट संरक्षण गर्न सरकार प्रतिवद्ध रहे तापनि सरकारले आत्मसुरक्षा (self protection) को महत्त्वका साथै व्यक्तिगत जिम्मेवारीमा पनि विशेष ध्यान दिन्छ।सरकारले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीका माध्यमबाट सूचना प्रसारण गरी आत्मसुरक्षामार्फत जोखिम न्यूनीकरणमा विशेष जोड दिनेछ।

७.३.२ सूचना तथा सञ्चार प्रविधि (ICT) प्रयोग गर्ने नेपालका प्रत्येक सरकारी संस्थाहरू तथा व्यवसायीहरूलाई व्यक्तिगत जोखिम आकलन (individual risk assessment) गर्न, मुख्य जोखिमहरूलाई सम्बोधन गर्ने साइबर सुरक्षा रणनीतिको विकास तथा कार्यान्वयन गर्न, उच्चस्तरीय व्यवस्थापनको पदाधिकारीलाई साइबर सुरक्षा प्रयास तथा पहलका लागि जिम्मेवारीका साथ मुख्य सूचना सुरक्षा अधिकृत तोक्न, साइबर सुरक्षा प्रयास तथा पहलका लागि जिम्मेवारी लिन, यसका जोखिम परिदृश्य (risk landscape) झल्काउने नवीनतम/अत्याधुनिक (state of act) साइबर सुरक्षा प्रविधि कायम राख्न, जोखिम आकलन तथा जोखिम व्यवस्थापन प्रक्रियाहरू कार्यान्वयन गर्न, व्यवसायको नियमित व्यवस्थापन र विपद् व्यवस्थापन (business continuity management and crisis management) योजना अन्तर्गत नियमित अभ्यास सञ्चालन गर्न अभिप्रेरित गरिनेछ। यसका अतिरिक्त संवेदनशील पूर्वाधार प्रदायकलाई अन्य आवश्यकताहरू लागू गर्न अभिप्रेरित गरिनेछ।

७.३.३ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले नेपालमा व्यवसायहरूका लागि स्तरीय जोखिम आकलन ढाँचाको विकास गर्नेछ। यस ढाँचाको प्रयोग गर्न नेपालका व्यवसायीहरूलाई अभिप्रेरित गरिनेछ।

७.३.४ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले साइबर सुरक्षासम्बन्धी सेवाहरू, उत्पादनहरू तथा प्रणालीहरू विकास गर्नाका साथै यसको मूल्याङ्कन र प्रमाणीकरण समेत गर्नेछ।

७.३.५ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले प्राविधिक तथा संस्थागत सुरक्षा उपायहरूको विकास एवं कार्यान्वयन गर्नाको साथै अत्यावश्यक सरकारी सेवाहरू (जस्तै e-government) लाई सुरक्षा गर्न आकस्मिक योजनाहरू तर्जुमा गर्नेछ।

७.३.६ नेपाल सरकारले साइबरसम्बन्धी अन्य जोखिमहरू तथा साइबर अपराधको अनुसन्धान, प्रतिरोधशक्ति एवं अभियोजन (prosecute) गर्ने क्षमताको सशक्तीकरण गरी राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीको माध्यमबाट साइबर सुरक्षाका उपायहरूको (measures) सुधारमा लक्ष्यित क्रियाकलापहरूलाई बढावा, पथ प्रदर्शन (guide) र समन्वय गर्नेछ।

७.४ नियमनकारी तथा कानूनी ढाँचाको सशक्तीकरण – राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली

७.४.१ सरकारले साइबर सुरक्षाका विषयहरूलाई सम्बोधन गर्न विद्युतीय कारोबार ऐन, २०६३ लागू गरेको छ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले साइबर सुरक्षासँग सम्बन्धित विद्यमान कानूनलाई कानून, न्याय तथा संसदीय मामिला मन्त्रालयको सुपरिवेक्षणमा पुनरावलोकन गर्नेछ। यसले कानूनका निम्नलिखित क्षेत्रहरूलाई संलग्न गर्नेछ :-

गोपनीयता तथा तथ्याङ्कको सुरक्षा (data protection),

राष्ट्रिय सुरक्षा, विद्युतीय व्यापार (e-commerce),

सूचनाको स्वतन्त्रता, विद्युतीय प्रमाणको ग्राह्यता (admissibility of electronic evidence), सेवा प्रदायकहरूको दायित्व,

बालबालिकाको अनलाइन सुरक्षा (children online protection) एवं अन्तर्राष्ट्रिय सहयोग आदि ।

पुनरावलोकनले साइबर सुरक्षाका सम्बन्धमा प्रयोग गर्न सकिने विद्यमान प्रावधानहरूको पहिचान, अन्तर्राष्ट्रिय उत्तम अभ्याससँगको तुलना, कमी कमजोरीको विश्लेषण (gap analysis), संशोधनका लागि सुझावहरू तथा सम्न्धित

मस्यौदा निर्देशनहरूलाई समेट्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले यस क्षेत्रमा क्रियाशील अन्तर्राष्ट्रिय संस्थाहरूको सहयोगको खोजी गर्नेछ।

७.४.२ साइबर अपराधका सम्बन्धमा निम्नलिखित विषयहरूलाई विश्लेषण गरिनेछः-

- परिभाषा, सारभूत फौजदारी कानून, कार्यविधि कानून, कानून कार्यान्वयनकारी निकायका अनुसन्धान सामग्रीहरू, सेवा प्रदायकहरूको दायित्व तथा अन्तर्राष्ट्रिय सहयोग।

७.५ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीको क्षमता वृद्धि

७.५.१ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले नेपालले फाइदा लिनसक्ने साइबर सुरक्षासँग सम्बन्धित क्षमतावृद्धि कार्यक्रमहरूको सूची (list) तयार गर्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले नदोहोरिने तरिकाबाट विभिन्न क्रियाकलापहरूलाई सूचीकृत गरी एउटा मार्गचित्र (road map) को विकास गर्नेछ जसले देशको आवश्यकता अनुरूप सम्भावित कार्यक्रमहरूको पहिचान तथा कुन कार्यक्रमहरूले कुन क्रियाकलापलाई समेट्छ भन्ने सुझावहरू दिन्छ।

७.५.२ प्राथमिक एवं उच्च विद्यालयका सबै विद्यार्थीहरूलाई कम्तीमा वर्षको एकपटक साइबर सुरक्षाका बारेमा नवीनतम प्रचलन (latest trend) सम्बन्धमा तालिम उपलब्ध गराउन शिक्षा मन्त्रालय, महिला, बालबालिका तथा समाज कल्याण मन्त्रालय र युवा तथा खेलकुद मन्त्रालयले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली तथा नेपालका अन्य निकायको सहकार्यमा पाठ्यक्रमको विकास गर्नेछन्। शिक्षकहरूका लागि तालिम सामग्री, पार्श्वसूचना (background information) तथा नमुना प्रस्तुतिहरू (sample presentations) को विकास गरिनेछ। यसका अतिरिक्त विद्यार्थीहरूलाई सूचना तथा सञ्चार प्रविधिको प्रयोग गर्न सक्षम बनाउनाका साथै विशेषतः बाल साइबर सुरक्षा जोखिमबारे जानकारी दिन विद्यालयहरूले प्रश्नावली (questionnaire) प्राप्त गर्नेछन्। वार्षिक रूपमा बेनामी आकलन (anonymous assessment) सञ्चालन गरिनेछ र यसको नतिजा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीसमक्ष प्रस्तुत गरी वार्षिक प्रतिवेदनमा समावेश गरिनेछ।

७.५.३ शिक्षा मन्त्रालय तथा विश्वविद्यालयहरूले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली र नेपालका अन्य निकायहरूसँगको सहकार्यमा सूचना प्रविधि (IT) सुरक्षा पेशाकर्मीहरू (IT) का लागि विशिष्टीकृत तालिम दिन पाठ्यक्रमको विकास गर्नेछ। यसको लक्ष्य नेपालमा सुरक्षासम्बन्धी मामिलाहरूलाई समाधान गर्नसक्ने सुरक्षा पेशाकर्मीहरू पर्याप्त मात्रामा उपलब्ध गराउनु हो।

७.५.४ कानून कार्यान्वयन गर्ने अधिकारीहरू, वित्तीय अनुसन्धान एकाइ, न्यायालय तथा अन्य सरोकारवालाहरूका लागि राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले साइबर अपराधसम्बन्धी एउटा दिगो तालिम कार्यक्रमको विकास गर्नेछ।

७.६ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीको सूचना आदानप्रदान

७.६.१ नागरिकहरू, व्यवसायीहरू र सरकारलाई साइबर घटनाहरूका बारेमा जानकारी गराउन अभिप्रेरित गरिनेछ। संवेदनशील राष्ट्रिय पूर्वाधार प्रदायकहरूलाई यस्ता जाहेरी/प्रतिवेदनहरू पेश गर्न बाध्यकारी बनाइनेछ।

७.६.२ सूचनाको आदानप्रदान (information sharing) का लागि राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले साइबर सुरक्षा घटनाहरूको सन्दर्भमा नवीनतम प्रचलनहरूको (recent trends) पहिचान (detect) गर्न, आकस्मिक स्तरको प्रणाली (emergency level system) सृजना गर्न, प्रतिवेदन ढाँचामा घटनाहरूको संक्षेपीकरण गर्न एवं सूचना (background information) उपलब्ध गर्नाका साथै यस्ता प्रतिवेदनहरू सम्बन्धित सूचना प्रणाली (channels) (जस्तैः प्रेस विज्ञप्तिहरू, ग्रामीण इलाकाहरूमा समन्वय, साझेदारहरूलाई पेश गरिएका सूचना) को विकास गरी त्यस्ता सूचनालाई पेश गर्ने कार्यतालिकाको विकास गर्नेछ। गोप्य राख्नु नपर्ने (non-confidential) सूचनालाई नियमित रूपमा सार्वजनिक पहुँच हुने वेबसाइटमा प्रकाशित गर्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले वर्षको एक पटक आफूले गरेको कार्यको संक्षिप्त प्रतिवेदन (summary report) तथा विशेष रूपले प्राप्त विज्ञप्तिहरू पेश गर्नुपर्नेछ। यसले सरकारलाई नियमित जानकारीहरू (briefings) उपलब्ध गराउनाका साथै माग बमोजिम अतिरिक्त सूचना प्रदान गर्नुपर्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले विभिन्न सरोकारवालाहरूलाई (stakeholders) सूचना उपलब्ध गराउँदा तिनीहरूको आवश्यकतालाई ध्यान दिनेछ। (उदाहरणार्थः मन्त्रीका लागि छोटकरी विवरण (executive summary), प्रणाली प्रशासक (administrator) का लागि विस्तृत प्राविधिक विवरण)। साथै, सम्प्रेषित सूचना उपलब्ध गराउँदा प्रभावित नभएकाहरूलाई सूचना वितरण गराइएको छैन भन्ने कुराको यकिन गर्नुपर्नेछ।

७.६.३ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले संभाव्य आपराधिक गतिविधि हुनसक्ने घटनाहरूका बारेमा कानून कार्यान्वयनकारी निकायहरूलाई जानकारी गराउनेछ। कानून कार्यान्वयनकारी निकायले सम्पर्कको एकल विन्दु (single point of contact) को व्यवस्था गर्नाका साथै राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले उपलब्ध गराएको सुरक्षित पूर्वाधारको प्रयोग गरिएको कुराको

यकिन गर्नुपर्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीद्वारा जाहेर भएका आपराधिक प्रकृतिका मामिलाहरू (cases) बारे अनुसन्धान गर्न सरकारले कानून कार्यान्वयनकारी निकायभित्रै एउटा उपयुक्त संरचनाको स्थापना गर्नेछ ।

७.६.४ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली तथा अन्य निकायबिच संवेदनशील एवं गोपनीय सूचनाको आदानप्रदानलाई सहज बनाउन राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सुरक्षित पूर्वाधार (secure infrastructure), सञ्चार, सूचना संकलनको प्रणाली स्थापना गर्नेछ र सम्भव भएसम्म यस्तो पूर्वाधारको माध्यमबाट मात्रै (exclusively) सूचनाको आदानप्रदान गरिनेछ।

७.६.५ मोबाइल सञ्चारका (mobile communication) फाइदाहरूलाई सरकारले मान्यता प्रदान गर्दछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले मोबाइल उपकरणहरूवाट (devices) आक्रमणहरूबारे जानकारी गराउन सकिने संभाव्यतालाई सक्षम बनाउनाका साथै नागरिकहरू र व्यवसायीहरूलाई नवीनतम आक्रमणहरूका बारेमा सूचना प्रवाह गर्न push services को प्रयोगको सम्भाव्यताको खोजी गर्नेछ।

७.७ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीसँग अन्तर्राष्ट्रिय सहयोग

७.७.१ अन्तर्राष्ट्रिय सहकार्यको सन्दर्भमा नेपालको कानूनी संरचना तथा अभ्यास पूर्ण रूपमा अन्तर्राष्ट्रिय उत्तम अभ्यास (international best practices) अनुरूप छ भन्ने यकिन गर्न राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले कानून, न्याय, तथा संसदीय मामिला मन्त्रालय र परराष्ट्र मन्त्रालयसँगको सहयोगमा देशका निकायहरूलाई समयमा नै जानकारी गराउनाका साथै कानूनी सहायतका लागि अनुरोध गर्ने सम्बन्धमा नेपालको क्षमताको विश्लेषण गर्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सम्पर्कको एकल विन्दु (single point of contact) स्थापनाका लागि सिफारिशहरूको विकास गर्नेछ। यसका अतिरिक्त राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले अनुरोधको प्राप्ति र प्रेषण (receiving and sending) का लागि प्रयोग हुने प्रविधिका साथै सम्पर्क विन्दु अन्तर्राष्ट्रिय उत्तम अभ्यास अनुरूप भए नभएको बारेमा विश्लेषण गर्नेछ।

७.७.२ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले अन्तर्राष्ट्रिय वा क्षेत्रीय संझौताहरूबारे जानकारी, नेपाल सहभागी हुनका लागि आवश्यक बाध्यात्मक मापदण्डको विकासका प्रक्रियाहरूका साथै २४/७ सञ्जाल (network) (जस्तैः इन्टरपोल सञ्जाल) का सम्बन्धमा सुझाउ/सिफारिसहरू दिनेछ। विद्यमान संयन्त्रको पहुँचको मूल्याङ्कनका सन्दर्भमा नेपालका लागि सान्दर्भिक कानुनी मापदण्ड तथा संस्कृतिसँग सम्बन्धित एवं अन्य देशहरूसँगको सहयोगको

उपयोगितालाई ध्यानमा राखिनेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले आवश्यकतानुसार विश्वव्यापी एवं क्षेत्रीय कम्प्युटर आपतकालीन पहल टोली (CERT) हरूको सदस्यता लिने प्रयास गर्नेछ।

७.७.३ साइबर सुरक्षाको संस्कारलाई प्रोत्साहन दिन तथा अन्तर्राष्ट्रिय दूरसञ्चार संघ (ITU) अनुरूप सूचना तथा सञ्चार प्रविधिको (ICT) प्रयोगमा सुरक्षा र विश्वसनीयता निर्माण गर्न राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले विश्वव्यापी साइबर सुरक्षा सूची अभ्यास (Global Cyber security Index Exercise) को सञ्चालन गर्नेछ।

८. बाल अनलाइन सुरक्षा (Child Online Protection)

८.१ निम्नलिखित पदाधिकारीहरू सम्मिलित बाल अनलाइन सुरक्षा कार्यसमूह (Child Online Protection Working Group– COPWG) को गठन गरिनेछ :-

सचिव, महिला, बालबालिका तथा समाज कल्याण मन्त्रालय	–अध्यक्ष
सहसचिव, सूचना तथा सञ्चार मन्त्रालय	–सदस्य
सहसचिव, शिक्षा मन्त्रालय	–सदस्य
नेपाल प्रहरी, महिला तथा बालबालिका निर्देशानालय प्रहरी नायव महानिरीक्षक -DIG	–सदस्य
प्रतिनिधि, राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (Nep CERT)	–सदस्य
प्रतिनिधि, नेपाल दूरसञ्चार प्राधिकरण	–सदस्य
प्रतिनिधि, बालबालिका सम्बन्धित संस्था	–सदस्य

८.२ बाल अनलाइन सुरक्षा कार्यसमूह (COPWG) ले बाल अनलाइन सुरक्षाका सम्बन्धमा ध्यान दिनुपर्ने आवश्यक क्षेत्रहरू (जस्तैः प्राविधिक सुरक्षा उपायहरू (measures), विद्यालयका लागि पाठ्यक्रम र आमाबुबा तथा अभिभावकहरूका लागि सूचना सामग्री) को पहिचान गर्नेछ।

८.३ बाल अनलाइन (children online) सुरक्षा गर्न सेवा प्रदायकहरूले अपनाउनुपर्ने विभिन्न प्राविधिक उपायहरूको मूल्याङ्कन बाल अनलाइन सुरक्षा कार्यसमूहले गर्नेछ। साथै, यदि अभिभावकहरूले अनुरोध गरेमा उपलब्ध गराउनुपर्ने प्रतिवेदनको मापदण्ड समेत मूल्याङ्कन गर्नेछ (हेर्नुहोस् ८.४)। मूल्याङ्कनको आधारमा बाल अनलाइन सुरक्षा कार्यसमूहले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (Nep CERT) सँगको सहकार्यमा बाल अनलाइन सुरक्षासम्बन्धी प्राविधिक मापदण्डको निर्देशिका तयार गर्नेछ। यसले सेवाको दुरुपयोगको रोकथाम सम्बन्धमा समेत सिफारिस/सुझाउहरू दिनेछ।

८.४ बाल अनलाइन सुरक्षा कार्यसमूहद्वारा तयार पारिएका निर्देशिकाको अधीनमा रही इन्टरनेट सेवा प्रदायकहरूले ग्राहकको अनुरोधमा त्यस्तो सेवा प्रदान गर्नुपर्नेछ जसमा बालबालिकाका लागि अनपयुक्त विषयवस्तु अवरुद्ध गर्न (block content) उपलब्ध प्राविधिक उपायहरू (technical measures) समाविष्ट हुनेछन्। यसका अतिरिक्त सेवा प्रदायकहरूले प्रयोगकर्ताको अनुरोधमा आमाबाबु वा अभिभावकहरूलाई विशेष प्रतिवेदन (special reporting) प्रदान गर्नुपर्नेछ जसमा प्रयोग गरेका सेवाहरू र बाल अनलाइन सुरक्षा कार्यसमूहद्वारा तय गरिएका अन्य विवरणहरू समावेश हुनुपर्नेछ।

८.५ नेपालका प्रत्येक मोबाइल सेवा प्रदायकले बाल अनलाइन सुरक्षा कार्यसमूहद्वारा तयार पारिएको निर्देशिकाको अधीनमा रही ग्राहकको अनुरोधमा बालबालिकाका लागि उपयुक्त नहुने सेवाहरूमा निषेधित पहुँच (restricted access) सहितको सिम कार्ड उपलव्ध गर्नुपर्नेछ। यी सेवाका लागि सेवा प्रदायकले थप शुल्कको माग नगर्न सक्दछ।

९. संवेदनशील पूर्वाधारको सुरक्षा

९.१. संवेदनशील पूर्वाधारको परिभाषा एवं वर्गीकरण

संवेदनशील पूर्वाधार भन्नाले स्वास्थ्य, सुरक्षा र नेपाली अर्थतन्त्रसँग सम्बन्धित सेवाका लागि आवश्यक पूर्वाधारलाई जनाउनेछ। संवेदनशील पूर्वाधारमा संलग्न क्षेत्रहरू; स्वास्थ्य सेवा र सार्वजनिक स्वास्थ्य क्षेत्र, ऊर्जा क्षेत्र, जल तथा अपविष्ट जल (waste water) क्षेत्र, यातायात क्षेत्र, सूचना तथा सञ्चार प्रविधि क्षेत्र, खाद्य तथा कृषि क्षेत्र, वित्तीय सेवा क्षेत्र, सरकारी सुविधा क्षेत्र, आकस्मिक सेवा क्षेत्र, कानून कार्यान्वयन तथा न्यायपालिका, रक्षा, संवेदनशील निर्माण सेवा एवं पर्यटन सेवामा मात्र सीमित रहने छैन। संवेदनशील पूर्वाधारको परिभाषा गर्ने सन्दर्भमा अन्तर्राष्ट्रिय उत्तम अभ्यासहरूलाई आधार मानिनेछ। कार्यदलले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीलाई देशमा रहेका संवेदनशील पूर्वाधार प्रदायकहरूको सूची उपलब्ध गराउनेछ।

९.१.१ सूचना तथा सञ्चार प्रविधिको बढ्दो प्रयोगसँगै नागरिकहरूको सूचना पूर्वाधारमा भरपर्ने क्रम बढ्नेछ। सञ्चालनमा हुने विफलता (failure) वा सीमित सञ्चालनले बहुसंख्यक नागरिकहरूमा व्यापक प्रभाव पार्नसक्ने हुँदा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीबाट वर्तमान बहुसंख्यक सूचना पूर्वाधारलाई संवेदनशील सूचना पूर्वाधारका रूपमा लिन सकिन्छ। संवेदनशील पूर्वाधार विरुद्धका संभावित आक्रमणहरू सूचना पूर्वाधारमा मात्र सीमित रहने छैनन् – विभिन्न संवेदनशील पूर्वाधार प्रदायकहरू जो सूचना पूर्वाधारसँग सम्बन्धित छैनन्, जस्तो कि विद्युत् तथा यातायात प्रदायकहरूले सूचना तथा सञ्चार प्रविधिको व्यापक रूपमा प्रयोग गर्दछन्। अतः व्यापक प्रभावको सम्बन्ध प्रत्यक्ष क्षतिसँग मात्र नभई अप्रत्यक्ष क्षतिसँग पनि हुन्छ। यस नीतिले सङ्ग्रहीत

(stored) वा प्रसारित (transmitted) डाटा वा नेटवर्क र सूचना प्रणालीको उपलब्धता, प्रामाणिकता, अखण्डता एवं विश्वसनीयता (availability, authenticity, integrity and confidentiality) को स्तर वृद्धि गर्न संवेदनशील पूर्वाधार प्रदायकहरूले सञ्चालन गरेको वा उपयोग गरेको सूचना प्रणालीका लागि सरकारले सञ्जालहरूको क्षमता वृद्धि गर्न आधार निर्माण गर्दछ।

९.१.२ संवेदनशील पूर्वाधार र साइबर जोखिमहरूका सम्बन्धमा विशेषतः संवेदनशील पूर्वाधार प्रदायकहरूको सुरक्षा सशक्त बनाउन सरकार कटिबद्ध रहनेछ। यसले संवेदनशील पूर्वाधार प्रदायकका साथै संवेदनशील पूर्वाधार प्रयोगकर्तालाई पनि समाहित गर्नेछ। कुनै बाध्यात्मक मापदण्डको कार्यान्वयन संवेदनशील पूर्वाधार संचालकहरूको क्षमताका साथै आवश्यकतामा आधारित भएको सुनिश्चित गर्न सरकारले साना तथा मध्यम उद्यमीहरु (SMEs), ठूला उद्यमीहरू र सार्वजनिक एवं निजी संवेदनशील पूर्वाधार प्रदायकहरूलाई ध्यानमा राखी आवश्यकता एवं जोखिमको आकलन (need and risk assessment गर्नेछ।

९.१.३ साइबर आक्रमण विरुद्ध संवेदनशील पूर्वाधारको दीर्घकालीन लचकता तथा स्थायित्वका लागि सम्बद्ध सबै निजी तथा सार्वजनिक सरोकारवालाहरू सम्मिलित क्षेत्रीय स्तरका साथै देशव्यापी बहस (debate) सञ्चालन गर्न सरकारले बढावा दिनेछ।

९.१.४ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले संवेदनशील पूर्वाधारको सुरक्षालाई ध्यान दिँदै निम्नलिखित कार्यहरू गर्नेछः-

- सूचना आदानप्रदान, रोकथाम तथा पूर्वचेतावनी (early warning)
- सुरक्षा प्रवर्धनमा केन्द्रित पहिचान (detection)
- प्रतिक्रिया (reaction)
- संकट व्यवस्थापन (crisis management)

पर्याप्त प्राविधिक, वित्तीय तथा जनशक्ति कायम गर्न तिनलाई सुम्पिएका जिम्मेवारी प्रभावकारी एवं कुशल तवरबाट (effective and efficient manners) सम्पादन गर्न र तदनुरूप यस नीतिगत लक्ष्यका उद्देश्य प्राप्तिका लागि यसले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीलाई आवश्यक कोषको व्यवस्था गरिनेछ। साइबर आक्रमणका सन्दर्भमा यसले संवेदनशील पूर्वाधार प्रदायकको आफ्नो दायित्वको अवज्ञा (non-compliance) तथा यसबाट संवेदनशील पूर्वाधारको सुरक्षामा परेको तत्सम्बन्धी प्रभावहरूको अनुसन्धान गर्न राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीलाई अधिकार प्रदान गर्नेछ। यसले विशेषतः राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीसँग संवेदनशील पूर्वाधार प्रदायकबाट

सुरक्षा नीतिहरू सम्बन्धी विवरणहरू लगायत तिनीहरूको सूचना प्रणाली एवं नेटवर्कहरूको सुरक्षाका सम्बन्धमा अपनाइएका विवरणहरू आवश्यकता अनुसार माग गर्नसक्ने अधिकार छ भन्ने यकिन गर्नेछ। यस सम्बन्धमा सरकारले यो सुनिश्चित गर्नेछ कि राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीसँग संवेदनशील पूर्वाधार प्रदायकहरूलाई बाध्यात्मक निर्देशन जारी गर्ने अधिकार हुनेछ। सरकारले यस नीति अन्तर्गत संवेदनशील पूर्वाधार प्रदायकमाथि लगाइएको (imposed) कुनै दायित्वमा न्यायिक पुनरावलोकन हुन सक्नेछ भन्ने कुराको यकिन गर्नेछ।

९.१.५ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (Nep CERT) लाई सरकारले प्राविधिक साइबर सुरक्षा निर्देशिका तर्जुमा गर्नका लागि संवेदनशील पूर्वाधार सम्बन्धित विषयहरूमा योगदान गर्न अनुरोध गर्नेछ। यस अतिरिक्त यसले साइबर घटनाहरूसँग संवेदनशील पूर्वाधार प्रदायकलाई सहयोग गर्न आवश्यक प्राविधिक तथा जनशक्तिहरूका साथै एउटा घटना व्यवस्थापन प्रणाली (incident management system) व्यवस्था गर्नुपर्नेछ। यस सहयोगको उद्देश्य संवेदनशील पूर्वाधार प्रदायकलाई चाहिने आवश्यक जनशक्तिको प्रतिस्थापन गर्नु नभई उनीहरूलाई अतिरिक्त सहयोग प्रदान गर्नु हो।

९.१.६ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले राष्ट्रिय आकस्मिक योजना (National Contingency Plan) को विकास गर्नेछ र बृहत् नेटवर्क सुरक्षा घटना पहल (large scale network security incident response) एवं विपद् पुनर्लाभ (disaster recovery) का लागि नियमित अभ्यासहरूको आयोजना गर्नेछ। यी अभ्यासहरूको आयोजना गर्दा यस क्षेत्रमा भएका नवीनतम प्रचलन र विकासलाई संलग्न गर्नुपर्नेछ, जसले गर्दा संवेदनशील पूर्वाधार प्रदायक कुनै पनि आक्रमण विरुद्ध प्राविधिक रूपमा तयार हुनेछ। आक्रमणका विरुद्ध तयारी गर्न, प्राविधिक तत्त्वहरूलाई (technical components) समाहित (cover) गर्न र जोखिम व्यवस्थापनका लागि संवेदनशील पूर्वाधार प्रदायकलाई इजाजत दिन नवीनतम प्रचलन र विकासलाई (latest trends and developments) संलग्न गर्नु पर्नेछ।

९.१.७ नेपालको कुन पूर्वाधार प्रदायकलाई **'संवेदनशील पूर्वाधार प्रदायक'** मान्ने भनी निर्धारण गर्न राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (Nep CERT) ले एउटा कार्यदलको गठन गर्नेछ।

९.१.८ सूचीमा (list) आधारित भई राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले संवेदनशील पूर्वाधार प्रदायकको डाटाबेस तयार गरी अद्यावधिक गर्नेछ। माग

गरिएका तथ्याङ्क उपलवब्ध गराउन संवेदनशील पूर्वाधारका प्रदायकहरू बाध्य हुनेछन्।डाटाबेसमा सेवा प्रदायकको विवरण तथा सेवा प्रदान गर्ने क्षेत्र (उदाहरणार्थ सेवा प्रयोग गर्ने घरधुरीहरूको संख्या), प्रयोग गरिएका सूचना तथा सञ्चार प्रविधि एवं मूलभूल सेवाहरूको (core services) सान्दर्भिकताका बारेमा समीक्षा (overview), जोखिमको आकलन (risk self-assessment), प्रत्युपाय (counter measure) (प्राविधिक तथा जोखिम व्यवस्थापन) र समीक्षा तथा पूर्व घटनाहरूको (previous incidents) सूचीका बारेमा सूचना समावेश भएको हुनुपर्दछ।

९.१.९ संवेदनशील पूर्वाधार प्रदायकहरूलाई राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले डाटाबेस अद्यावधिक गर्न कम्तीमा वर्षको एक पटक प्रश्नावली उपलवब्ध गराउनेछ।उल्लिखित तथ्याङ्कका अतिरिक्त राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सुरक्षा स्तरहरूको उद्देश्य तथा विस्तारको सीमाका साथै सुरक्षासम्बन्धी मापदण्ड एवं तिनलाई पालना गर्नका लागि प्रयोग भएका विधिहरूका बारेमा सूचना माग गर्न सक्नेछ।

९.१.१० संवेदनशील पूर्वाधार प्रदायकहरूका नेटवर्क एवं सूचना प्रणालीहरूमा भएका जोखिमहरूको व्यवस्था गर्न प्राविधिक र संगठनात्मक उपायहरू अपनाउनु आवश्यक छ।आधुनिकता (state of art) लाई मध्यनजर राख्दै यी उपायहरूले संभावित जोखिमहरूलाई उचित सुरक्षास्तरको प्रत्याभूति गर्नुपर्नेछ।विशेषतः तिनीहरूले प्रदान गर्ने सेवा, नेटवर्क तथा सूचना प्रणालीमा हुनसक्ने घटनाहरूको असर रोक्ने र न्यूनीकरण गर्ने उपायहरूको अवलम्बन गरिनु पर्दछ र यसरी ती नेटवर्कहरू तथा सूचना प्रणालीद्वारा प्रदान गरिने सेवाहरूको निरन्तरताको यकिन गर्नुपर्दछ।संवेदनशील पूर्वाधार प्रदायकले क्रियाकलापहरूको समन्वय गर्न उच्चस्तरीय व्यवस्थापनका सदस्यलाई प्रमुख सूचना सुरक्षा अधिकृतका रूपमा नियुक्त गर्नुपर्नेछ र यसले साइबर सुरक्षा उपायहरूको कार्यान्वयनका लागि निश्चित बजेटको व्यवस्था गरिएको छ भन्ने कुराको सुनिश्चित गर्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले स्थानीय आवश्यकता पहिचान गरी आय तथा कर्मचारीहरू र ग्राहकहरूको कुल संख्याका आधारमा संस्थागत कम्प्युटर आपतकालीन पहल टोली (CERTs) को (organizational CERTs) सृजना र स्थापनाको लागि सुझाव गर्नेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीसँग संवेदनशील पूर्वाधारका प्रदायकहरूका संस्थागत कम्प्युटर आपतकालीन पहल टोली (CERT) ले समन्वय र सूचना आदानप्रदान गर्नुपर्नेछ।यसका अतिरिक्त संवेदनशील पूर्वाधार प्रदायकले कम्तीमा वर्षको एक

पटक जोखिम तथा यसबाट हुनसक्ने प्रभावका बारेमा मूल्याङ्कन गरी यस प्रक्रियालाई लेखवद्ध (document) गर्नु पर्नेछ। राष्ट्रिय अभ्यासहरूका अतिरिक्त तिनीहरूले कम्तीमा वर्षको एकपटक यथार्थपरक अभ्यास (realistic exercise) कार्यक्रम सञ्चालन गर्नुपर्दछ जसले वास्तविक आक्रमणको समयमा प्रयोग हुने प्राविधिक उपायहरू र नवीनतम (state of art) एवं जोखिम व्यवस्थापन प्रक्रियाहरू (risk management processes) पर्याप्त छन् भनी जाँच गर्न प्रदायकलाई मद्दत मिल्नेछ।

९.१.११ सरकारले आकलनको विश्लेषण (analysis of assessment) गरी भविष्यमा बाध्यात्मक न्यूनतम मापदण्डहरू (mandatory minimum standards) लागू गरिनुपर्ने वा नपर्ने भन्ने कुराको निर्णय गर्नेछ। यस सन्दर्भका विकासको गति, साना र ठूला प्रदायकका विभिन्न क्षमता एवं कुनै ठोस मापदण्डहरूको आवश्यक सुधारका बारेमा सरकार सचेत हुनेछ।

९.१.१२ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले निर्देशिका तयार गर्नुका साथै कुशल सुरक्षालाई बढावा दिई प्रगतिको व्यवस्था एवं अनुगमन गर्न सक्नेछ। यसको साथै राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले प्राकृतिक र विद्वेशात्मक आक्रमण (natural and malicious threat) बाट पुनर्लाभ (recovery) लगायतका तयारी (preparedness) मा प्रयोग हुने विधिहरू तयार गर्न सक्नेछ।

९.१.१३ सरकारले संवेदनशील पूर्वाधारका प्रदायकका लागि प्रमाणीकरणको व्यवस्था लागू गर्ने सम्बन्धमा विचार गर्नेछ र यसमा सम्बन्धित संभाव्यता अध्ययन (related feasibility study) समेत गर्नेछ।

९.१.१४ सूचना आदानप्रदान साइबर आक्रमण विरुद्ध लड्ने विभिन्न उपायहरूमध्ये एक हो। संवेदनशील पूर्वाधार प्रदायकको नेटवर्कमा हुनसक्ने साइबर आक्रमणका बारेमा बुझ्नको लागि राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले यस सम्बन्धमा सान्दर्भिक सूचना संकलन गर्नेछ। सोही समयका संवेदनशील पूर्वाधारका प्रदायकका साथै सरकार एवं सरकारी संस्थाहरूलाई विशेषतः साइबर आक्रमण विरुद्ध तयारीको अवस्था (status of readiness), घटनाहरू (status of readiness), प्रचलन (trends) र विकासका बारेमा आवश्यक सूचना उपलब्ध गराउने जिम्मेवारी राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीको हुनेछ। सरकारले राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीलाई संवेदनशील पूर्वाधारका सम्बन्धमा सूचना आदानप्रदान गर्न तथा साइबर सुरक्षाको सम्बन्धमा असल नीतिका बारेमा जानकारी उपलब्ध गराउन लागि राष्ट्रिय मञ्च (national

forum) को स्थापना गर्न अनुरोध गर्नेछ। यस मञ्चमा संवेदनशील पूर्वाधार प्रदायक, सरकारी संस्थाहरू, कानून कार्यान्वयन गर्ने निकाय, नागरिक समाज तथा अन्य रुचि राख्ने पक्षलाई सम्मिलित गर्नु पर्दछ। यसका साथै सुरक्षा तथा लचकता (security and resilience) उद्देश्यहरू, न्यूनतम आवश्यकता (baseline requirements), असल नीति अभ्यासहरू (good policy practices) र उपायहरूका सम्बन्धमा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले निजी तथा सार्वजनिक क्षेत्रबिच सहकार्य गर्न विशेष कार्य सञ्चालन गर्नेछ।

९.१.१५ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सार्वजनिक, निजी, अनुसन्धान एवं विकास परियोजनाको माध्यमबाट संवेदनशील पूर्वाधारको साइबर सुरक्षाको सुधारको संभावनाको अध्ययन गनुपर्नेछ।

९.१.१६ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले जागरुकता बढाउने रणनीति (awareness raising strategy) को विकास तथा कार्यान्वयन गर्नाका साथै देशभित्रका संवेदनशील पूर्वाधार प्रदायकसम्म पहुँच बनाउनेछ।

९.१.१७ देशभित्र जारी (ongoing) विकासका सम्बन्धमा सूचनामा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीको पहुँच भएको यकिन गर्न, संवेदनशील पूर्वाधार प्रदायकहरूले तिनले प्रदान गर्ने मूल सेवाहरूको (core services) सुरक्षामा महत्त्वपूर्ण प्रभाव भएको सूचना तथा सञ्चार प्रविधि (ICT) सँग सम्बन्धित कुनै घटनाहरूका बारेमा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीलाई सुरक्षित पूर्वाधारको माध्यमबाट सूचित गर्नुपर्नेछ। तत्सम्बन्धमा राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले निर्देशिका तर्जुमा गर्न सक्नेछ। आवश्यकतानुसार कुन परिस्थितिमा संवेदनशील पूर्वाधार प्रदायकहरूले घटना सम्बन्धमा सूचित गर्न आवश्यक छ भन्ने बारेमा निर्देशन जारी गर्न सक्नेछ। यसका अतिरिक्त राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले प्रतिवेदनका लागि आवश्यक ढाँचा र प्रक्रियाहरुको तर्जुमा गर्नेछ। सरकारले यस नीतिको आशय अनुरूप सूचनाको आदानप्रदान गर्नेमा विशेष जोड दिनेछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले संकलित सूचनाको विश्लेषण गर्नाका साथै सूचना बाँड्ने र विशेषतः घटनाको चेतावनी (incident warning) का लागि सूचनाको प्रयोग गर्नेछ। जहाँ घटनाको खुलासा (disclosure) सार्वजनिक हितमा छ भनी यसले निश्चय गर्दछ, त्यहाँ यसले सर्वसाधारणलाई सूचित गर्दछ वा संवेदनशील पूर्वाधार प्रदायकलाई सो गर्न लगाउँदछ। राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले घटनाका बारेमा अन्य संवेदनशील पूर्वाधार प्रदायकलाई जानकारी गराउन सक्नेछ। यदि निकट भविष्यमा यस प्रकारको घटना अन्य संवेदनशील पूर्वाधार

प्रदायकलाई पनि लक्षियित गर्नसक्ने संभावना भएमा र यस्तो सूचनाको आदानप्रदानबाट अन्य संभाव्य प्रभावित संवेदनशील पूर्वाधार प्रदायकलाई समान रूपको आक्रमणबाट बचाउन मद्दत गर्ने भएमा प्रतिवेदन प्रेषकको हितको संरक्षणलाई ध्यानमा राखी राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले सूचना आदानप्रदान गर्नुपूर्व सम्भव भएसम्म सूचनाहरू बेनामी (anonymized) रहून् भन्ने कुराको सुनिश्चितता गर्नेछ।

९.१.१८ राष्ट्रिय कम्प्युटर आपतकालीन पहल टोलीले संवेदनशील पूर्वाधार विरुद्धका साइबर आक्रमणका साथै राष्ट्रिय जोखिम व्यवस्थापन प्रक्रियाहरूसँग (national risk management processes) सम्बन्धित नीति तथा कानूनको नियमित रूपमा पुनरावलोकन गर्नेछ।

१०. नीतिगत ढाँचाको कार्यान्वयन

१०.१ निम्नलिखित संरचनासहित सूचना तथा सञ्चार मन्त्रालयमा एउटा राष्ट्रिय साइबर सुरक्षा नीति कार्यान्वयन सञ्चालन समितिको (National Cyber Security Policy Implementation Steering Committee) गठन गरिनेछ :-

मन्त्री, सूचना तथा सञ्चार मन्त्रालय	अध्यक्ष
सचिव, सूचना तथा सञ्चार मन्त्रालय	सदस्य
सचिव, गृह मन्त्रालय	सदस्य
सचिव, विज्ञान तथा प्रविधि मन्त्रालय	सदस्य
सचिव, महिला बालबालिका तथा समाज कल्याण मन्त्रालय	सदस्य
सचिव, अर्थ मन्त्रालय	सदस्य
अध्यक्ष, नेपाल दूरसञ्चार प्राधिकरण	सदस्य

१०.२ नीतिका प्रावधानहरूको प्रभावकारी कार्यान्वयनसँगै नीतिका व्यवधानहरू (policy interventions) को अनुगमन तथा मूल्याङ्कनका लागि समन्वय प्रदान गर्नु नै राष्ट्रिय साइबर सुरक्षा नीति कार्यान्वयन सञ्चालन समितिको प्रमुख भूमिका हुनेछ।

१०.३ समितिले नीतिगत प्रावधानहरूको क्रियान्वयनका सम्बन्धमा डोमेनसँग सम्बन्धित सुझाव एवं सिफारिसहरू प्रदान गर्न निजी क्षेत्रसहित डोमेन विज्ञहरु (domain experts) तथा सरोकारवाला समुदायको प्रतिनिधित्व हुने गरी एउटा साइबर सुरक्षा कार्यान्वयन उपसमितिको गठन गर्नेछ।

११. राष्ट्रिय सूचना तथा सञ्चार प्रविधि गुरुयोजना/राष्ट्रिय विद्युतीय रणनीतिको स्थापना

नेपाल सरकारबाट स्वीकृत/प्रमाणित हुने राष्ट्रिय साइबर सुरक्षा गुरुयोजनामार्फत नीति तथा रणनीति ढाँचाको कार्यान्वयन गरिनेछ।

१२. स्रोत परिचालन

निजी तथा सार्वजनिक दुवै क्षेत्रको स्रोतहरूको परिचालनमार्फत साइबर सुरक्षा नीतिका समग्र लक्ष्यहरूको प्राप्ति गरिनेछ। प्रस्तावित नीतिगत ढाँचाले सुरक्षित वातावरणमा निजी तथा सार्वजनिक क्षेत्रको भविष्यको लगानीको आधार सृजना गर्ने अपेक्षा गरिएको छ। द्विपक्षीय, बहुपक्षीय तथा अन्य अन्तर्राष्ट्रिय निकायबाट प्राप्त हुने संभावित अनुदान तथा प्राविधिक सहयोगको पनि उपयोग गर्न सकिनेछ।

१३. कानुनी प्रबन्धहरू

प्रस्तुत नीति तथा यसका प्रावधानहरू कार्यान्वयनका लागि आवश्यकता अनुसार उपयुक्त कानुनी तथा नियमनकारी प्रबन्धहरूको निर्माण गरिनेछ।

१४. अनुगमन तथा मूल्याङ्कन

साइबर सुरक्षा नीतिको कार्यान्वयनका लागि नियमित अनुगमन तथा मूल्याङ्कन गर्न आर्थिक वर्ष आ.व २०७३/०७४ भित्र अनुगमन तथा मूल्याङ्कन ढाँचाको विकास गरिनेछ। साइबर सुरक्षासँग सम्बन्धित कार्यक्रम तथा नीतिका प्रावधानहरूको अनुगमन तथा मूल्याङ्कन कार्य सम्पादन गर्नु कार्यान्वयन सञ्चालन समितिको प्रमुख उत्तरदायित्व हुनेछ।

❖