सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा व्यवस्था गर्न बनेको विधेयक

प्रस्तावना: सूचना प्रविधिको विकास, प्रबर्द्धन र नियमन गर्न, विद्युतीय अभिलेख तथा हस्ताक्षरको मान्यता, सत्यता र विश्वसनीयतालाई नियमित गर्न, विद्युतीय माध्यमबाट सार्वजनिक सेवा प्रवाह गर्ने सम्बन्धमा साइबर स्पेसमा सङ्कलित, सङ्ग्रहित, प्रशोधित, प्रकाशित वा प्रसारित सूचना, तथ्याङ्क एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको गोपनीयता, अखण्डता, उपलब्धता, प्रमाणिकता र आधिकारिकता कायम राख्न, संवेदनशील सूचना पूर्वाधारको पहिचान तथा सुरक्षा गर्न, सूचना प्रविधि तथा साइबर सुरक्षा सेवा प्रदायकलाई नियमन गर्न, अनुसन्धान गर्न र यस क्षेत्रमा हुने अपराध नियन्त्रण गर्ने सम्बन्धमा व्यवस्था गर्न प्रचलित कानूनलाई संशोधन र एकीकरण गर्न वाञ्छनीय भएकोले,

संघीय संसदले यो ऐन बनाएको छ।

परिच्छेद—१

प्रारम्भिक

1. **संक्षिप्त नाम, विस्तार र प्रारम्भ**: (१) यस ऐनको नाम "सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी ऐन, २०८०" रहेको छ।

(२) यो ऐन तुरुन्त प्रारम्भ हुनेछ।

(३) यो ऐन नेपालभर लागू हुनेछ र नेपालबाहिर बसी नेपाल वा नेपाली नागरिक विरुद्ध यस ऐन बमोजिमको कसूर गर्ने व्यक्तिको हकमा समेत लागू हुनेछ।

2. **परिभाषा**: विषय वा प्रसङ्गले अर्को अर्थ नलागेमा यस ऐनमा,-

(क) "अनुमतिपत्र" भन्नाले साइबर सुरक्षा सेवा प्रदान गर्नका लागि साइबर सुरक्षा सेवा प्रदायकलाई दफा ९८ बमोजिम दिइने अनुमतिपत्र सम्झनु पर्छ।

(ख) "अनुसन्धान अधिकृत" भन्नाले दफा १४१ बमोजिम तोकिएको अनुसन्धान अधिकृत सम्झनु पर्छ।

(ग) "उत्पत्तिकर्ता" भन्नाले विद्युतीय अभिलेख उत्पन्न गर्ने, भण्डारण गर्ने वा सम्प्रेषण गर्ने व्यक्ति सम्झनु पर्छ र सो शब्दले त्यस्तो कार्य अन्य कुनै व्यक्तिलाई गर्न लगाउने व्यक्ति समेतलाई जनाउँछ।

(घ) "कम्प्युटर" भन्नाले विद्युतीय स्वरुपमा रहेको तथ्याङ्कलाई प्रशोधन तथा भण्डारण गर्न सकिने कुनै पनि विद्युतीय उपकरण सम्झनु पर्छ।

(ङ) "कम्प्युटर प्रणाली" भन्नाले आगत र निर्गत (इन्पुट र आउटपुट) सहायता संयन्त्र लगायतका कम्प्युटर कार्यक्रम, विद्युतीय निर्देशन, आगत र निर्गत तथ्याङ्कहरु समाविष्ट भएको र तार्किक, अङ्कगणितीय, तथ्याङ्क सञ्चय तथा पुनः प्राप्ति, सञ्चार र नियन्त्रण लगायतका कार्यहरू सम्पादन गर्ने संयन्त्र वा संयन्त्रको समूह सम्झनु पर्छ।

(च) "केन्द्र" भन्नाले दफा ९४ बमोजिमको राष्ट्रिय साइबर सुरक्षा केन्द्र सम्झनु पर्छ।

(छ) "कम्प्यूटर प्रोग्राम" भन्नाले तथ्याङ्क प्रशोधन गर्न निर्देशन दिने वा कुनै विद्युतीय आदेश वा आदेशको समूह जसलाई कम्प्यूटरमा प्रयोग गरिएमा कुनै निश्चित कार्य गर्न सकिने कुरा सम्झनु पर्छ।

(ज) "क्लाउड सेवा" भन्नाले वेब प्रविधिको माध्यमबाट प्रयोगकर्ताको माग बमोजिम क्लाउड कम्प्युटिङ्ग सेवा प्रदायकबाट प्राप्त हुने सूचना प्रविधिसँग सम्बन्धित पूर्वाधार लगायतका सबै प्रकारका सेवा सम्झनु पर्छ।

(झ) "जोडी साँचो" (की पीयर) भन्नाले डिजिटल हस्ताक्षर सिर्जना गर्ने निजी साँचो र सो हस्ताक्षर सम्पुष्टि गर्ने गणितीय रुपमा अन्तरआबद्ध सार्वजनिक साँचोको जोडी सम्झनु पर्छ।

(ञ) "डोमेन नाम" भन्नाले इन्टरनेटको माध्यमबाट वेबसाईटमा पहुँच पुऱ्याउनको लागि प्रदान गरिने वेबसाईटको ठेगाना सम्झनु पर्छ।

(ट) "डाटा सेन्टर" भन्नाले डाटा भण्डारण, व्यवस्थापन, प्रशोधन र आदानप्रदान गर्नको लागि उच्च क्षमताको कम्प्युटर पूर्वाधार जस्तै सर्भर, राउटर, स्विच, फायरवाल, स्टोरेज र अन्य सुविधा लगायतको अग्नि नियन्त्रण प्रणाली, वातावरण अनुकूलन व्यवस्थापन प्रणाली जस्ता सुविधाहरु रहेको संरचना सम्झनु पर्छ।

(ठ) "डिजिटल हस्ताक्षर" भन्नाले दफा २० को उपदफा (१) बमोजिमको शर्त पूरा गरी विद्युतीय स्वरुपमा भएको हस्ताक्षर सम्झनु पर्छ।

(ड) "तथ्याङ्क" भन्नाले कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कमा प्रयोग गर्ने उद्देश्यले अक्षर, अंक, छवि, ध्वनि वा श्रव्य दृश्यमा औपचारिक तवरले तयार पारिदै गरेको वा तयार गरिएको वा कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कद्वारा उत्पादन गरिएको सूचना, ज्ञान तथा अवधारणा वा निर्देशनको प्रस्तुतीकरण सम्झनु पर्छ।

(ढ) "तोकिएको" वा "तोकिए बमोजिम" भन्नाले यस ऐन अन्तर्गत बनेको नियममा तोकिएको वा तोकिए बमोजिम सम्झनु पर्छ।

(ण) "निजी साँचो" (प्राईभेट की) भन्नाले डिजिटल हस्ताक्षर सृजना गर्न प्रयोग गरिएको जोडी साँचो मध्ये सम्बन्धित प्रयोगकर्तासँग मात्र रहने साँचो सम्झनु पर्छ।

(त) "नियन्त्रक" भन्नाले दफा २४ बमोजिम नियुक्त भएको वा तोकिएको नियन्त्रक सम्झनु पर्छ।

(थ) "निर्देशक समिति" भन्नाले दफा ३ बमोजिमको साइबर सुरक्षा निर्देशक समिति सम्झनु पर्छ।

(द) "न्यायाधिकरण" भन्नाले दफा १५१ बमोजिम गठन भएको सूचना प्रविधि न्यायाधिकरण सम्झनु पर्छ।

(ध) "पहुँच" (एक्सेस) भन्नाले कुनै कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कको तार्किक, अङ्गगणितीय वा स्मरण कार्य सम्पदाहरुमा प्रवेश प्राप्त गर्ने, त्यस्ता सम्पदाहरुलाई निर्देशन दिने वा त्यस्ता सम्पदाहरुसँग सञ्चार सम्पर्क गर्न सक्ने अवसर सम्झनु पर्छ।

(न) "प्रमाणपत्र" भन्नाले दफा ४३ बमोजिम प्रमाणीकरण निकायले जारी गरेको डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र सम्झनु पर्छ।

(प) "प्रयोगकर्ता" भन्नाले डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र प्राप्त गरेको व्यक्ति सम्झनु पर्छ।

(फ) "प्रमाणीकरण निकाय" भन्नाले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्न दफा २६ बमोजिम इजाजतपत्र प्राप्त प्रमाणीकरण निकाय सम्झनु पर्छ।

(ब) "मन्त्रालय" भन्नाले नेपाल सरकारको सूचना प्रविधि सम्बन्धी विषय हेर्ने मन्त्रालय सम्झनु पर्छ।

(भ) "व्यक्ति" भन्नाले प्राकृतिक व्यक्ति वा कानून बमोजिम दर्ता भएको कुनै कम्पनी, फर्म वा संस्था सम्झनु पर्छ।

(म) "विभाग" भन्नाले नेपाल सरकारको सूचना प्रविधि सम्बन्धी विषय हेर्ने विभाग सम्झनु पर्छ।

(य) "विद्युतीय अभिलेख" भन्नाले कम्युटर तथा कम्प्युटर प्रणालीको प्रयोग गरी डिजिटल ढाँचामा राखिने सबै किसिमका अभिलेख सम्झनु पर्छ।

(र) "विद्युतीय प्रणाली" भन्नाले अन्तरआवद्ध वा आपसमा सम्बन्धित विद्युतीय उपकरण वा उपकरणहरुको समूह सम्झनु पर्छ र सो शब्दले एक वा एक भन्दा बढि उपकरण विद्युतीय तथ्याङ्क वा सिग्नलको स्वचालित रुपमा प्रशोधन (अटोमेटिक प्रोसेसिङ्ग) गर्ने कार्य र स्थायी, अस्थायी वा अन्य त्यस्तै विद्युतीय भण्डारण माध्यमलाई समेत जनाउँछ।

(ल) "वैयक्तिक विवरण" भन्नाले कुनै पनि व्यक्तिको देहायको विषयसँग सम्बन्धित सूचना वा विवरण सम्झनु पर्छः—

(१) निजको जात, जाति, जन्म, उत्पत्ति, धर्म, वर्ण वा वैवाहिक स्थिति,

(२) निजको शिक्षा वा शैक्षिक उपाधि,

(३) निजको ठेगाना, टेलिफोन वा इमेलको ठेगाना वा अन्य कुनै विद्युतीय पहिचान,

(४) निजको राहदानी, नागरिकताको प्रमाणपत्र, राष्ट्रिय परिचयपत्र नम्बर, सवारी चालक अनुमतिपत्र, मतदाता परिचयपत्र वा सरकारी निकायबाट जारी भएका परिचयपत्रको विवरण,

(५) वैयक्तिक सूचना उल्लेख गरी निजले कसैलाई पठाएको वा निजले प्राप्त गरेको पत्र,

(६) निजको औलाको छाप, हस्तरेखा, आँखाको रेटिना, रगत समूह वा निजको अन्य जैविक विवरण,

(७) निजको अपराधिक पृष्ठभूमि वा निजले फौजदारी कसूरमा सजाय पाएको वा कसूर भुक्तान गरेको विवरण,

(८) कुनै निर्णय प्रक्रियामा पेशागत वा विशेषज्ञ राय दिने व्यक्तिले त्यस्तो प्रक्रियामा के, कस्तो राय वा धारणा व्यक्त गरेको थियो भन्ने विषय,

(व) "सफ्टवेयर" भन्नाले कम्प्युटर हार्डवेयर सञ्चालन गर्ने क्षमता भएको सिष्टम सफ्टवेयर र एप्लिकेशन सफ्टवेयर जस्ता कम्प्युटर प्रणालीको कुनै खास अंश सम्झनु पर्छ।

(श) "समन्वय समिति" भन्नाले दफा ६ बमोजिमको सूचना प्रविधि तथा साइबर सुरक्षा समन्वय समिति सम्झनु पर्छ।

(ष) "सरकारी निकाय" भन्नाले नेपाल सरकारको मन्त्रालय, सचिवालय वा सो अन्तर्गतका कार्यालय, संवैधानिक निकाय वा सो अन्तर्गतका कार्यालय, अदालत, प्रदेश सरकार वा सो अन्तर्गतका कार्यालय, स्थानीय तह र सो अन्तर्गतका कार्यालय सम्झनुपर्छ र सो शब्दले त्यस्तै प्रकृतिका अन्य कार्यालय समेतलाई जनाउँछ।

(स) "साइबर सुरक्षा" भन्नाले कम्प्यूटर वा कम्प्यूटर प्रणालीमा भण्डारण वा प्रशारण हुने सामग्रीको गोपनीयता तथा अखण्डता कायम गरी सुरक्षित राख्ने तथा कम्प्यूटर वा कम्प्यूटर प्रणालीलाई निरन्तर रुपमा उपयोग र सञ्चालन गर्न अनाधिकृत पहुँच वा साइबर आक्रमणबाट सुरक्षित राख्न अपनाइने सुरक्षा सम्झनु पर्छ।

(ह) "साइबर सुरक्षा जोखिम "भन्नाले कम्प्यूटर वा कम्प्यूटर प्रणालीमा रहेको कमजोरी वा अन्य कुनै कारणले एक कम्प्यूटर वा कम्प्यूटर प्रणाली मार्फत अर्को कम्प्यूटर वा कम्प्यूटर प्रणालीको साइबर सुरक्षामा पार्न सक्ने अनधिकृत पहुँच वा जोखिमलाई सम्झनु पर्छ।

(क्ष) "साइबर सुरक्षा घटना" भन्नाले कानूनसम्मत अधिकार बिना कुनै कम्प्यूटर वा कम्प्यूटर प्रणाली मार्फत अर्को कम्प्यूटर वा कम्प्यूटर प्रणालीको साइबर सुरक्षामा जोखिम निम्त्याउने, नकारात्मक प्रभाव पार्ने वा क्षति पुऱ्याउने कार्य सम्झनु पर्छ।

(त्र) "साइबर सुरक्षा सेवा" भन्नाले अनुसूची-१ बमोजिमको साइबर सुरक्षा सेवा सम्झनु पर्छ।

(ज्ञ) "साइबर सुरक्षा सेवा प्रदायक" भन्नाले साइबर सुरक्षा सेवा प्रदान गर्ने व्यक्ति वा संस्था सम्झनु पर्छ।

(कक) "सार्वजनिक साँचो" (पब्लिक की) भन्नाले डिजिटल हस्ताक्षरको सम्पुष्टि गर्न प्रयोग गरिएको कुनै जोडी साँचोको एक साँचो सम्झनु पर्छ।

(कख) "सार्वजनिक संस्था" भन्नाले देहायका संस्था सम्झनु पर्छः—

(१) नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहको पूर्ण वा आंशिक स्वामित्व वा नियन्त्रणमा रहेको कम्पनी, बैङ्क वा समिति, संस्था वा प्रचलित कानून बमोजिम स्थापित आयोग, संस्था, प्राधिकरण, निगम, प्रतिष्ठान, बोर्ड, केन्द्र, परिषद् र यस्तै प्रकृतिका अन्य सङ्गठित संस्था,

(२) नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहद्वारा सञ्चालित वा नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहको पूर्ण वा आंशिक अनुदानप्राप्त विश्वविद्यालय, विद्यालय, अनुसन्धान केन्द्र र अन्य त्यस्तै प्राज्ञिक वा शैक्षिक संस्था,

(३) नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहको ऋण, अनुदान वा जमानतमा सञ्चालित संस्था,

(४) उपखण्ड (१) वा (२) वा (३) मा उल्लिखित संस्थाको पूर्ण वा आंशिक स्वामित्व भएको वा नियन्त्रण रहेको वा त्यस्तो संस्थाबाट अनुदानप्राप्त संस्था,

(५) नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहले राजपत्रमा सूचना प्रकाशन गरी सार्वजनिक संस्था भनी तोकेको अन्य संस्था।

(कग) "सूचना" भन्नाले सरकारी निकाय, सार्वजनिक संस्था वा कुनै व्यक्ति तथा संस्थाबाट सम्पादन हुने वा भएको महत्वपूर्ण काम, कारबाही वा निर्णयसँग सम्बन्धित कुनै तथ्याङ्क सम्झनु पर्छ।

(कघ) "सूचना प्रविधि" भन्नाले कम्प्युटर तथा कम्प्युटर प्रणालीको प्रयोग गरिएका सबै स्वरुपका सूचना, सृजना गर्ने, उत्पादन गर्ने, सम्प्रेषण गर्ने, प्राप्त गर्ने वा सुरक्षण गर्ने प्रविधि सम्झनु पर्छ।

(कङ) "सूचना प्रविधि प्रणाली" भन्नाले कम्प्युटर प्रणाली वा विद्युतीय प्रणाली प्रयोग गरी सूचना सृजना गर्ने, उत्पादन गर्ने, सम्प्रेषण गर्ने, प्राप्त गर्ने, जम्मा गर्ने, प्रदर्शन गर्ने वा अन्य किसिमबाट प्रशोधन गर्ने हार्डवेयर, सफ्टवेयर तथा नेटवर्क सहितको प्रणाली सम्झनु पर्छ।

(कच) "सेवा प्रदायक" भन्नाले कुनै तेस्रो पक्षको सूचना आदान प्रदान वा भण्डारण गर्ने कार्य गर्ने व्यक्ति सम्झनु पर्छ।

(कछ) "संवेदनशील सूचना पूर्वाधार" भन्नाले दफा १०४ बमोजिम तोकिएको संवेदनशील सूचना पूर्वाधार सम्झनु पर्छ।

(कज) "संवेदनशील सूचना पूर्वाधारको धनी" भन्नाले संवेदनशील सूचना पूर्वाधारको स्वामित्व प्राप्त व्यक्ति वा संस्था सम्झनु पर्छ र सो शब्दले त्यस्तो संवेदनशील सूचना पूर्वाधारको धनी एक भन्दा बढी भएमा प्रत्येक धनी समेतलाई जनाउँछ।

परिच्छेद-२

सूचना प्रविधि तथा साइबर सुरक्षा संरचना सम्बन्धी व्यवस्था

3. निर्देशक समितिको गठन : (१) सूचना प्रविधि तथा साइबर सुरक्षाको क्षेत्रमा आवश्यक निर्देशन एवं समन्वय गर्न देहाय बमोजिमको निर्देशक समिति रहनेछः-

(क)	सञ्चार तथा सूचना प्रविधि मन्त्री	-अध्यक्ष
(ख)	गभर्नर, नेपाल राष्ट्र बैङ्क	-सदस्य
(ग)	सचिव, अर्थ मन्त्रालय	-सदस्य
(घ)	सचिव, गृह मन्त्रालय	-सदस्य
(ङ)	सचिव, रक्षा मन्त्रालय	-सदस्य
(च)	सचिव, शिक्षा, विज्ञान तथा प्रविधि मन्त्रालय	-सदस्य
(छ)	सचिव, संचार तथा सूचना प्रविधि मन्त्रालय	-सदस्य
(ज)	अध्यक्ष, नेपाल दूरसञ्चार प्राधिकरण	-सदस्य
(झ)	नेपाल उद्योग वाणिज्य महासङ्घका अध्यक्ष	

(ञ) सूचना प्रविधि वा साइबर सुरक्षाको क्षेत्रमा कम्तीमा पन्ध्र वर्ष काम गरी ख्यातिप्राप्त व्यक्तिहरुमध्येबाट मन्त्रालयले मनोनयन गरेको एकजना महिला समेत तीन जना -सदस्य

(ट) सह-सचिव, मन्त्रालय -सदस्य-सचिव

4. **<u>निर्देशक समितिको काम, कर्तव्य अधिकार:</u>** निर्देशक समितिको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) समन्वय समितिवाट पेश भएका सूचना प्रविधि तथा साइबर सुरक्षाका लागि अवलम्बन गर्नुपर्ने अल्पकालीन तथा दीर्घकालीन नीति स्वीकृतिका लागि नेपाल सरकार समक्ष सिफारिस गर्ने,

(ख) सूचना प्रविधि तथा साइबर सुरक्षा सुदृढ गर्नका लागि समन्वय समितिवाट पेश भएको प्रचलित कानूनमा आवश्यक सुधारका विषयमा नेपाल सरकार समक्ष सिफारिस गर्ने,

(ग) समन्वय समितिवाट पेश भएको सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी प्राविधिक मापदण्ड स्वीकृत गर्ने,

(घ) समन्वय समितिको सिफारिस बमोजिम सूचना प्रविधि तथा साइबर सुरक्षाका लागि विभिन्न निकायहरुबीच समन्वय, सहजीकरण र सहकार्य गर्ने,

(ङ) मानवीय वा प्राकृतिक कारणले हानी नोक्सानी पुगी राष्ट्रिय सुरक्षा, अर्थव्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य वा सार्वजनिक सुरक्षासँग सम्बन्धित सूचना प्रविधि प्रणाली सञ्चालन अवरुद्ध भएमा समन्वय समितिलाई आवश्यक पर्ने सहजीकरण गर्ने,

(च) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा प्रदेश, स्थानीय तह तथा अन्य सम्बद्ध निकाय बीच आवश्यक समन्वय गर्ने,

(छ) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी अन्य कार्यहरुमा आवश्यकता अनुसार सहजीकरण गर्ने ।

5. **<u>निर्देशक समितिको बैठकः</u>** (१) निर्देशक समितिको बैठक आवश्यकता अनुसार वर्षको कम्तीमा एक पटक बस्नेछ।

(२) निर्देशक समितिको बैठक सो समितिको अध्यक्षले तोकेको मिति, समय र स्थानमा बस्नेछ।

(३) निर्देशक समितिको कुल सदस्य सङ्ख्याको पचास प्रतिशतभन्दा बढी सदस्यहरु उपस्थित भएमा निर्देशक समितिको बैठकको लागि गणपूरक सङ्ख्या पुगेको मानिनेछ।

(४) निर्देशक समितिको बैठकको अध्यक्षता समितिको अध्यक्षले गर्नेछ।

(५) निर्देशक समितिले आवश्यकता अनुसार सम्बन्धित विषयको विशेषज्ञलाई समितिको बैठकमा आमन्त्रण गर्न सक्नेछ।

(६) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि मानवीय वा प्राकृतिक कारणले राष्ट्रिय सुरक्षा, अर्थव्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य सेवा वा सार्वजनिक सुरक्षासँग सम्बन्धित सूचना प्रविधि प्रणालीको सञ्चालन अवरुद्ध भएमा निर्देशक समितिको बैठक जुनसुकै बखत बस्न सक्नेछ।

6. **<u>समन्वय समिति गठन:</u>** (१) राष्ट्रियस्तरको सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी घटनामा तत्काल प्रतिकार्य र सहायता प्रदान गर्नका लागि देहाय बमोजिमको सूचना प्रविधि तथा साइबर सुरक्षा समन्वय समिति रहनेछ:-

(क) सहसचिव, मन्त्रालय	-संयोजक
(ख) सूचना प्रविधि निर्देशक, प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय	-सदस्य
(ग) सूचना प्रविधि निर्देशक, अर्थ मन्त्रालय	-सदस्य
(घ) सूचना प्रविधि निर्देशक, गृह मन्त्रालय	-सदस्य
(ङ) सूचना प्रविधि निर्देशक, शिक्षा विज्ञान तथा प्रविधि मन्त्रालय	-सदस्य
(च) सूचना प्रविधि निर्देशक, संघीय मामिला तथा सामान्य प्रशासन मन्त्रालय	-सदस्य
(छ) सूचना प्रविधि हेर्ने सूचना प्रविधि निर्देशक, मन्त्रालय	-सदस्य
(ज) सूचना प्रविधि निर्देशक, सूचना प्रविधि विभाग	-सदस्य
(झ) सूचना प्रविधि निर्देशक, केन्द्र	-सदस्य
(ञ) सूचना प्रविधि निर्देशक, एकिकृत डाटा व्यवस्थापन केन्द्र	-सदस्य
(ट) सूचना प्रविधि निर्देशक, प्रमाणिकरण नियन्त्रकको कार्यालय	-सदस्य
(ठ) नेपाल प्रहरी, साइबर व्यूरोका प्रमुख वा निजले तोकेको प्रतिनिधि	-सदस्य
(ड) नेपाल राष्ट्र बैङ्कको अधिकृतस्तरको प्रतिनिधि	-सदस्य
(ढ) नेपाली सेनाको अधिकृतस्तरको प्रतिनिधि	-सदस्य
(ण) नेपाल दूरसञ्चार प्राधिकरणको अधिकृतस्तरको प्रतिनिधि	-सदस्य
(त) साइवर सुरक्षा हेर्ने सूचना प्रविधि निर्देशक, मन्त्रालय,	-सदस्य-सचिव

(२) समन्वय समितिको बैठकमा सम्बन्धित विषय विज्ञलाई आमन्त्रण गर्न सकिनेछ।

7. **<u>समन्वय समितिको काम, कर्तव्य र अधिकार</u>**: यस ऐनमा अन्यत्र उल्लेख गरिएका काम, कर्तव्य र अधिकारको अतिरिक्त समन्वय समितिको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः

(क) मानवीय तथा प्राकृतिक कारणले हानी नोक्सानी पुगी राष्ट्रिय सुरक्षा, अर्थव्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य वा सार्वजनिक सुरक्षासँग सम्बन्धित सूचना प्रविधि प्रणाली बन्द भएमा यथाशीघ्र सो प्रणालीलाई पुनः सञ्चालनमा ल्याउन सहायता गर्ने,

(ख) साइबर सुरक्षा सम्बन्धी घटनाको विस्तृत अध्ययन तथा विश्लेषण गरी सम्बन्धित निकाय वा व्यक्तिलाई जानकारी गराउने तथा सोको समाधानको लागि सहजीकरण गर्ने,

(ग) आवश्यकता अनुसार विषयगत तथा क्षेत्रगत सहायता समूहसँग सहजीकरण गर्ने,

(घ) क्षेत्रगत सहायता समूहको काम कारबाहीको अनुगमन गर्ने, गराउने,

(ङ) क्षेत्रगत समन्वय समितिको गठन, कार्यक्षेत्र र सञ्चालन सम्बन्धी कार्यविधि बनाई निर्देशक समिति समक्ष पेश गर्ने,

(च) संवेदनशील सूचना पूर्वाधारको सुरक्षाको लागि संवेदनशील सूचना पूर्वाधारको धनीलाई आवश्यकता अनुसार सहयोग प्रदान गर्ने,

(छ) साइबर आक्रमण भएको अवस्थामा आपतकालीन कार्यहरू गर्ने,

(ज) भविष्यमा हुन सक्ने साइबर सुरक्षा सम्बन्धी जोखिमबाट बच्नको लागि रणनीति तथा कार्ययोजना तयार गरी निर्देशक समिति समक्ष पेस गर्ने,

(झ) तोकिएका अन्य कार्य गर्ने।

परिच्छेद—३

विद्युतीय अभिलेख सम्बन्धी व्यवस्था

8. **विद्युतीय अभिलेखले कानूनी मान्यता पाउनेः** प्रचलित कानूनमा कुनै सूचना, लिखत, अभिलेख, तथ्याङ्क, लिखित वा मुद्रित वा अन्य कुनै स्वरुपमा हुनु पर्ने भनी उल्लेख गरिएको रहेछ भने त्यस्तो विषय यो ऐन वा यस ऐन अन्तर्गत बनेको नियममा उल्लिखित प्रक्रिया पूरा गरी विद्युतीय अभिलेखको रुपमा राखिएको अभिलेखले कानूनी मान्यता प्राप्त गर्नेछ।

9. **मूल वा सक्कल अभिलेखको रुपमा पेश गर्न सकिनेः** (१) प्रचलित कानूनमा मूल वा सक्कल अभिलेख नै पेश गर्नुपर्ने वा सुरक्षित राख्नु पर्ने भनी उल्लेख गरिएको रहेछ भने देहाय बमोजिमका शर्त पूरा भएमा त्यस्तो मूल वा सक्कल अभिलेखको विद्युतीय प्रति पेश गर्न सकिनेछः-

(क) विद्युतीय स्वरुपमा सृजना गरिएको समयदेखि सो अभिलेखमा कुनै पनि किसिमबाट परिवर्तन गरिएको छैन भनी विश्वास गर्न सकिने तोकिए बमोजिमको आधार विद्यमान भएमा,

(ख) त्यस्तो अभिलेखलाई कुनै व्यक्ति समक्ष पेश गर्नु पर्ने गरी अनिवार्य गरिएको अवस्थामा सो अभिलेखलाई जसका समक्ष पेश गरिनु पर्ने हो, सो व्यक्तिलाई स्पष्ट रुपमा देखाउन सकिने प्रकृतिको भएमा।

(२) उपदफा (१) बमोजिम पेश गरिएको अभिलेखले कानूनी मान्यता प्राप्त गर्नेछ।

10. **सुरक्षित राख्नु पर्ने** : (१) प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेख कुनै खास अवधिसम्म सुरक्षित राख्नु पर्ने भनी उल्लेख गरिएको रहेछ भने देहायका शर्त पूरा हुने गरी त्यस्तो सूचना, लिखत, तथ्याङ्क वा अभिलेख विद्युतीय स्वरुपमा सुरक्षित राख्नु पर्नेछ र त्यस्तो सूचना, लिखत, तथ्याङ्क वा अभिलेखले कानूनी मान्यता प्राप्त गर्नेछः-

(क) पछिल्ला प्रसङ्ग (रिफरेन्स)को रुपमा प्रयोग गर्न सकिने गरी पहुँचयोग्य अवस्थामा राखिएको भएमा,

(ख) शुरुमा सिर्जना गरी सम्प्रेषण गरिएको, प्राप्त गरिएको वा जम्मा गरिएको अवस्थाकै रुपमा पुनः दुरुस्त रुपमा प्रस्तुत गर्ने गरी प्रदर्शन गर्न सकिने ढाँचामा सुरक्षित राखिएको भएमा,

(ग) उत्पत्ति, गन्तव्य र सम्प्रेषण वा प्राप्तिको मिति तथा समय पहिचान गर्न सकिने विवरण उपलब्ध हुने गरी राखिएको भएमा।

(२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि कुनै अभिलेख सम्प्रेषण गर्ने वा प्राप्त गर्ने प्रयोजनको लागि स्वचालित रुपमा सिर्जना हुने सूचनाको सम्बन्धमा यस दफाको व्यवस्था लागू हुने छैन।

11. **<u>सुरक्षित विद्युतीय अभिलेख</u>** : तोकिए बमोजिमको सुरक्षण कार्यविधि अपनाई सृजना गरिएको विद्युतीय अभिलेखमा कुनै किसिमको हेरफेर गरिएको छ वा छैन भन्ने कुराको सम्बन्धमा तोकिए बमोजिम परीक्षण गरिएको भए त्यस्तो विद्युतीय अभिलेखलाई सुरक्षित विद्युतीय अभिलेख मानिनेछ।

12. **<u>उत्पत्तिकर्ताको अभिलेख मानिने</u>**: (१) देहायका अवस्थामा कुनै विद्युतीय अभिलेख उत्पत्तिकर्ताको अभिलेख मानिनेछः—

(क) उत्पत्तिकर्ता आफैले त्यस्तो विद्युतीय अभिलेख सम्प्रेषण गरेको भएमा,

(ख) त्यस्तो विद्युतीय अभिलेखको सम्बन्धमा आवश्यक कार्य गर्न उत्पत्तिकर्ताको तर्फबाट अख्तियारी प्राप्त गरेको व्यक्तिले त्यस्तो विद्युतीय अभिलेख सम्प्रेषण गरेको भएमा,

(ग) उत्पत्तिकर्ताको नियन्त्रणमा रहेको स्वचालित रुपमा सञ्चालन हुने गरी बनाइएको सूचना प्रविधि प्रणालीबाट त्यस्तो विद्युतीय अभिलेख सम्प्रेषण गरिएको भएमा।

(२) उपदफा (१) बमोजिम सम्प्रेषण गरिएको विद्युतीय अभिलेखको सम्बन्धमा तोकिए बमोजिमको अवस्था विद्यमान भएमा प्रापकले त्यस्तो विद्युतीय अभिलेख उत्पत्तिकर्ताको हो भन्ने कुरा मानी सोही आधारमा तत्सम्बन्धी कार्य गर्ने अधिकार प्राप्त गर्नेछ।

13. **<u>विद्युतीय अभिलेखको प्राप्ति र स्वीकार तथा सोको जानकारी दिने प्रकृया</u>**: (१) उत्पत्तिकर्ताले विद्युतीय अभिलेख पठाउँदाका बखत वा पठाउनुभन्दा अगावै प्रापकलाई सो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई पठाउन अनुरोध गरेको वा त्यसरी सूचना वा भरपाई पठाउन प्रापक र उत्पत्तिकर्ताका बीचमा सहमति भएको अवस्थामा त्यस्तो विद्युतीय अभिलेखको प्राप्ति स्वीकार गर्ने सम्बन्धमा उपदफा (२), (३) र (४) का व्यवस्थाहरु लागू हुनेछन्।

(२) विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई कुनै खास ढाँचामा वा कुनै खास तरिकाबाट दिनु पर्ने गरी उत्पत्तिकर्ता र प्रापकबीचमा कुनै सम्झौता नभएको अवस्थामा त्यस्तो सूचना वा भरपाई देहाय बमोजिम दिन सकिनेछः-

(क) प्रापकबाट स्वचालित वा अन्य कुनै किसिमको सञ्चार माध्यमद्वारा,

(ख) विद्युतीय अभिलेख प्राप्त भएको कुरा उत्पत्तिकर्तालाई सङ्केत गर्न पर्याप्त हुने किसिमको प्रापकको कुनै कार्यद्वारा।

(३) उत्पत्तिकर्ताले कुनै विद्युतीय अभिलेखको सम्बन्धमा त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्रापकबाट प्राप्त गरेपछि मात्र निजको हकमा त्यस्तो विद्युतीय अभिलेख बन्धनकारी हुने भनी उल्लेख गरेको अवस्थामा प्रापकबाट त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्राप्त नभएसम्म त्यस्तो विद्युतीय अभिलेख उत्पत्तिकर्ताले पठाएको मानिने छैन।

(४) उत्पत्तिकर्ताले कुनै विद्युतीय अभिलेखको सम्बन्धमा त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्रापकबाट प्राप्त गरेपछि मात्र निजको हकमा त्यस्तो विद्युतीय अभिलेख बन्धनकारी हुने भनी उल्लेख नगरेको अवस्थामा त्यस्तो विद्युतीय अभिलेख प्राप्तिको सूचना वा भरपाईको सम्बन्धमा उत्पत्तिकर्ता वा प्रापकबीच

कुनै समय निर्धारण वा मञ्जुरी नभएको भए तोकिए बमोजिमका समयभित्र उत्पत्तिकर्ताले प्रापकबाट त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्राप्त गरिसकेको हुनु पर्नेछ।

(५) उपदफा (४) बमोजिम प्रापकबाट विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्राप्त नभएमा त्यस्तो विद्युतीय अभिलेख उत्पत्तिकर्ताले पठाएको मानिने छैन।

(६) विद्युतीय अभिलेखको प्राप्ति, स्वीकार तथा सोको जानकारी दिने सम्बन्धी अन्य प्रक्रिया तोकिए बमोजिम हुनेछ।

14. **सम्प्रेषण र प्राप्तिको समय तथा स्थान**: (१) उत्पत्तिकर्ता र प्रापकबीचमा अन्यथा सम्झौता भएकोमा बाहेक कुनै विद्युतीय अभिलेख उत्पत्तिकर्ताको नियन्त्रण बाहिरको सूचना प्रविधि प्रणालीमा प्रवेश गरेपछि त्यस्तो विद्युतीय अभिलेखको सम्प्रेषण भएको मानिनेछ।

(२) उत्पत्तिकर्ता र प्रापकबीचमा अन्यथा सम्झौता भएकोमा बाहेक कुनै विद्युतीय अभिलेखको प्राप्तिको समय र स्थान तोकिए बमोजिम निर्धारण गरिनेछ।

15. **करारले कानूनी मान्यता पाउने** : प्रचलित कानून बमोजिम भएको करार यो ऐन वा यस ऐन अन्तरगत बनेको नियमको अधीनमा रहि विद्युतीय माध्यमबाट सम्पन्न भएको रहेछ भने त्यस्तो करारले कानूनी मान्यता पाउनेछ।

16. **सम्झौताद्वारा व्यवस्था गर्न सक्ने**: विद्युतीय अभिलेख सृजना गर्ने, सम्प्रेषण गर्ने, प्राप्त गर्ने, सञ्चय गर्ने वा अन्य कुनै किसिमबाट प्रशोधन गर्ने कार्यमा संलग्न पक्षहरुले तत्सम्बन्धी आफ्ना काम कारबाहीका सम्बन्धमा यस परिच्छेदका व्यवस्थाहरुको प्रतिकूल नहुने गरी सम्झौताद्वारा थप व्यवस्था गर्न सक्नेछन्।

17. **सूचना प्रविष्ट गर्न, हेरफेर गर्न, मेटाउन वा लुकाउन छिपाउन नहुने**: कसैले कुनै अप्रमाणिक विद्युतीय सूचनालाई प्रमाणिक हो भन्ने देखाउन वा कानूनी प्रयोजनको लागि प्रयोग गर्न पढ्न वा बुझ्न सकिने वा नसकिने जुनसुकै स्वरुपमा कुनै सूचना प्रविष्ट गर्न, हेरफेर गर्न, मेटाउन वा लुकाउन छिपाउन हुदैन।

18. **आर्थिक लाभ पु-याउने नियतले विद्युतीय प्रणालीको कार्य सञ्चालनमा हस्तक्षेप गर्न नहुने**: कसैले आफू वा अरु कसैलाई आर्थिक लाभ पु-याउने नियतले अनाधिकृत रुपमा विद्युतीय सूचना प्रविष्ट वा सम्प्रेषण वा हेरफेर गरी वा मेटाई वा लुकाई-छिपाई गरी विद्युतीय प्रणालीको कार्य सञ्चालनमा हस्तक्षेप गर्न वा कसैलाई आर्थिक नोक्सानी हुने गरी निजको संवेदनशील वित्तीय सूचना प्राप्त गर्न वा गराउन हुदैन।

19. **दुराशययुक्त प्रोग्राम संप्रेषण वा सञ्चालन गर्न नहुने:** कसैले विद्युतीय प्रणालीमा रहेको सूचना अनाधिकृत रुपमा प्राप्त गर्ने, परिवर्तन गर्ने, मेटाउने वा निष्क्रिय पार्ने उद्देश्यले कुनै प्रतिकूल प्रभाव पार्ने प्रोग्राम संप्रेषण गर्न वा सञ्चालन गर्न हुदैन।

20. **डिजिटल हस्ताक्षर**: (१) डिजिटल हस्ताक्षर सृजना गर्न देहाय बमोजिमका शर्त पूरा भएको हुनु पर्नेछः-

(क) हस्ताक्षरको सिर्जना सम्बन्धी तथ्याङ्क र प्रमाणीकरण तथ्याङ्क हस्ताक्षरकर्तासँग मात्र सम्बन्धित भएको यकिन गर्न सकिने भएमा,

(ख) हस्ताक्षरको सिर्जना सम्बन्धी तथ्याङ्क हस्ताक्षर गर्दाको बखतमा हस्ताक्षरकर्ताको मात्र नियन्त्रणमा रहेको पुष्टि गर्न सकिने भएमा,

(ग) विद्युतीय हस्ताक्षर गरिसकेपछि सम्बन्धित अभिलेख तथा हस्ताक्षरमा गरिएको परिवर्तन भए नभएको पत्ता लगाउन सकिने भएमा।

(२) यस परिच्छेदमा भएका व्यवस्थाहरुको अधीनमा रही प्रयोगकर्ताले निजको डिजिटल हस्ताक्षर प्रयोग गरी विद्युतीय अभिलेख प्रमाणित गर्न सक्नेछ।

21. **डिजिटल हस्ताक्षरको कानूनी मान्यता** : (१) प्रचलित कानूनमा कुनै सूचना, लिखत, अभिलेख वा अन्य कुनै कुरालाई हस्ताक्षरद्वारा प्रमाणित गर्नु पर्ने वा कुनै लिखतमा कुनै व्यक्तिको हस्ताक्षर गरिएको हुनु पर्ने भनी उल्लेख गरिएको रहेछ भने त्यस्ता सूचना, लिखत वा अभिलेख यो ऐन वा यस ऐन अन्तर्गत बनेको नियममा उल्लिखित प्रक्रिया पूरा गरी डिजिटल हस्ताक्षरद्वारा प्रमाणित गरिएको भए त्यस्तो डिजिटल हस्ताक्षरले कानूनी मान्यता प्राप्त गर्नेछ।

(२) उपदफा (१) बमोजिमको डिजिटल हस्ताक्षर सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

22. **सुरक्षित डिजिटल हस्ताक्षर मानिने**: कुनै विद्युतीय अभिलेखमा गरिएको डिजिटल हस्ताक्षरलाई तोकिए बमोजिमको सुरक्षण कार्यविधि अपनाई तोकिए बमोजिम परीक्षण र सम्पुष्टि गरिएको भए त्यस्तो डिजिटल हस्ताक्षरलाई सुरक्षित डिजिटल हस्ताक्षर मानिनेछ।

23. **विद्युतीय हस्ताक्षरको शुल्क निर्धारण:** विद्युतीय हस्ताक्षरको शुल्क सम्बन्धी व्यवस्था तोकिए बमोजिम हुनेछ।

24. **नियन्त्रक सम्बन्धी व्यवस्था**: (१) प्रमाणीकरण निकायलाई इजाजतपत्र दिने काम समेतको लागि नेपाल सरकारले तोकेको सेवा / समूहको राजपत्राङ्कित प्रथम श्रेणीको अधिकृतलाई नियन्त्रकको रुपमा नियुक्त गर्न सक्नेछ।

(२) नेपाल सरकारले नियन्त्रकको छुट्टै कार्यालय खोल्न सक्नेछ।

25. **नियन्त्रकको काम, कर्तव्य र अधिकार**: नियन्त्रकको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः -

(क) प्रमाणीकरण निकायलाई इजाजतपत्र प्रदान गर्ने,

(ख) प्रमाणीकरण निकायको काम कारबाहीको सुपरिवेक्षण र रेखदेख गर्ने,

(ग) प्रमाणीकरण निकायले डिजिटल हस्ताक्षरको सम्पुष्टि गर्ने सम्बन्धमा कायम गर्नु पर्ने स्तर निर्धारण गर्ने,

(घ) प्रमाणीकरण निकायले आफ्नो कारोबार सञ्चालन गर्दा पालन गर्नु पर्ने शर्त निर्धारण गर्ने,

(ङ) प्रमाणपत्रको ढाँचा र त्यसभित्र समाविष्ट हुनु पर्ने विषय वस्तुको निर्धारण गर्ने,

(च) प्रमाणीकरण निकायले यस परिच्छेद बमोजिम प्रकट गरेका सूचनाहरुको अभिलेख खडा गरी सार्वजनिक रुपमा पहुँचयोग्य हुने गरी तथ्याङ्कको व्यवस्था गर्ने र सो तथ्याङ्कलाई अद्यावधिक गर्ने,

(छ) प्रमाणीकरण निकायको वार्षिक कार्य सम्पादन परीक्षण गर्ने, गराउने,

(ज) एस.एस.एल.(सेक्युर्ड सकेट लेयर) सर्टिफिकेट जस्ता डिजिटल सर्टिफिकेट सम्बन्धी कार्य गर्ने,

(झ) तोकिए बमोजिमको अन्य काम गर्ने।

26. **प्रमाणीकरण निकाय सम्बन्धी व्यवस्था**: (१) डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्ने, निलम्बन गर्ने वा रद्द गर्ने काम समेतको लागि प्रमाणीकरण निकायले नियन्त्रकबाट यस ऐन बमोजिम इजाजतपत्र प्राप्त गर्नु पर्नेछ।

(२) उपदफा (१) मा जुनसुकै कुरा उल्लेख भए तापनि सार्वजनिक निकायको लागि डिजिटल हस्ताक्षरको प्रमाणपत्र जारी गर्न, निलम्वन वा रद्द गर्न नेपाल सरकारले प्रमाणीकरण निकायको रुपमा कुनै सरकारी निकायलाई तोक्न सक्नेछ।

(३) प्रमाणीकरण निकायको अन्य काम, कर्तव्य र अधिकार तोकिए बमोजिम हुनेछ।

27. <u>इजाजतपत्रको लागि निवेदन दिनु पर्नेः</u> (१) दफा २६ बमोजिम प्रमाणीकरण निकायको रुपमा काम गर्न तोकिए बमोजिमको योग्यता पुगेका व्यक्तिले इजाजतपत्र प्राप्त गर्न तोकिए बमोजिमको ढाँचामा तोकिए बमोजिमको दस्तुर सहित देहाय बमोजिमका कागजात सहित नियन्त्रक समक्ष निवेदन दिनु पर्नेछ :-

(क) प्रमाणीकरण सम्बन्धी विवरण,

(ख) निवेदकको पहिचान तथा सनाखतको पुष्टि हुने किसिमका कागजात,

(ग) वित्तीय स्रोत खुल्ने कागजात,

(घ) जनशक्ति तथा आवश्यक अन्य सुविधा खुल्ने कागजात,

(ङ) तोकिए बमोजिमका अन्य कागजात।

(२) दफा २७ को उपदफा (२) बमोजिमका सरकारी निकायलाई उपदफा (१) को खण्ड (ग) बमोजिमको कागजात आवश्यक पर्ने छैन।

28. <u>इजाजतपत्र दिनु पर्नेः</u> (१) नियन्त्रकले दफा २७ बमोजिम इजाजतपत्रको लागि आफू समक्ष प्राप्त भएको निवेदनको सम्बन्धमा तोकिए बमोजिमको योग्यता पुगे नपुगेको आवश्यक जाँचबुझ तथा मूल्यांकन गरी तोकिएको ढाँचामा इजाजतपत्र दिनु पर्नेछ।

(२) उपदफा (१) बमोजिमको इजाजतपत्रको विवरण सार्वजनिक रुपमा प्रकाशित गर्नुपर्नेछ।

(३) इजाजतपत्र सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

29. <u>इजाजतपत्र नवीकरण गर्नु पर्ने</u>ः (१) प्रमाणीकरण निकायले प्राप्त गरेको इजाजतपत्र प्रत्येक वर्ष नवीकरण गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिम इजाजतपत्रको नवीकरण गर्न चाहने प्रमाणीकरण निकायले तोकिए बमोजिमको ढाँचामा तोकिए बमोजिमको नवीकरण दस्तुर संलग्न गरी इजाजतपत्रको अवधि समाप्त हुनुभन्दा कम्तीमा दुई महिना अघि नियन्त्रक समक्ष निवेदन दिनु पर्नेछ।

(३) उपदफा (२) बमोजिम नवीकरणको लागि निवेदन पर्न आएमा नियन्त्रकले इजाजतपत्र नवीकरण गर्ने वा नगर्ने भन्ने सम्बन्धमा तोकिए बमोजिमको प्रक्रिया पूरा गरी इजाजतपत्रको अवधि समाप्त हुनुभन्दा एक महिना अघि निर्णय गरिसक्नु पर्नेछ।

(४) उपदफा (३) बमोजिम नवीकरण गर्ने वा नगर्ने सम्बन्धी निर्णय गर्दा दफा ३७ बमोजिमको कार्य सम्पादन परीक्षण प्रतिवेदन समेतलाई आधार लिन सकिनेछ।

(५) नियन्त्रकले इजाजतपत्र नवीकरण नगर्ने निर्णय गर्नु अघि निवेदकलाई आफ्नो सफाई पेश गर्ने मनासिब माफिकको मौका दिनु पर्नेछ।

30. <u>इजाजतपत्र निलम्बन गर्न सक्ने</u>: (१) प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्नको लागि नियन्त्रक समक्ष पेश गरेको कागजात वा विवरण र वित्तीय तथा भौतिक स्रोत फरक वा झुट्टा भएमा वा कारोबार सञ्चालन गर्दा पालन गर्नु पर्ने शर्तको पालना नगरेमा वा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको उल्लंघन गरेको पाइएमा नियन्त्रकले तत्सम्बन्धमा जाँचबुझ पूरा नभएसम्मका लागि प्रमाणीकरण निकायको इजाजतपत्र निलम्बन गर्न सक्नेछ।

तर त्यसरी इजाजतपत्र निलम्बन गर्नु अघि प्रमाणीकरण निकायलाई आफ्नो भनाई पेश गर्ने मनासिब माफिकको मौका दिनु पर्नेछ।

(२) इजाजत प्राप्त प्रमाणीकरण निकाय एउटा मात्र भई निलम्बनमा परेमा सो सम्बन्धी काम नियन्त्रकको कार्यालयले गर्नेछ।

(३) उपदफा (२) बमोजिम निलम्बन भएको अवस्थामा निलम्बनमा परेको संस्थाले प्रमाणीकरण कार्यको लागि प्रयोगमा रहेका हार्डवेयर, सफ्टवेयर, सूचना प्रविधि प्रणाली र सो सँग सम्बन्धित तथ्याङ्क नियन्त्रकलाई बुझाउनु पर्नेछ।

(४) उपदफा (२) बमोजिम निलम्बन भएको अवस्थामा निलम्बनमा परेको संस्थाबाट प्रमाणीकरण कार्यको लागि प्रयोगमा रहेका हार्डवेयर, सफ्टवेयर, सूचना प्रविधि प्रणाली र सो सँग सम्बन्धित तथ्याङ्क नियन्त्रकले प्राप्त गरि नियन्त्रकको कार्यालय मार्फत सञ्चालन गर्नु पर्नेछ।

(५) उपदफा (१) बमोजिमको निलम्बन उपर चित्त नबुझेमा सम्बन्धित व्यक्तिले सूचना प्रविधि न्यायाधिकरणमा पुनरावेदन गर्न सक्नेछ।

(६) इजाजतपत्र निलम्बन गर्ने सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

31. <u>इजाजतपत्र रद्द गर्न सक्ने</u>: (१) प्रमाणीकरण निकायको काम कारबाहीका सम्बन्धमा तोकिए बमोजिमको रीत पुऱ्याई भएको जाँचबुझबाट देहायका कुनै कुरा हुन गएको देखिएमा नियन्त्रकले यस ऐन बमोजिम जारी गरेको इजाजतपत्र जुनसुकै बखत रद्द गर्न सक्नेछ :-

(क) यो ऐन वा यस ऐन अन्तर्गत बनेको नियम अन्तर्गत पूरा गर्नु पर्ने दायित्व प्रमाणीकरण निकायले पूरा नगरेमा,

(ख) प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्नको लागि निवेदन दिंदाका बखत वा इजाजतपत्र नवीकरणको लागि निवेदन दिंदाका बखत झुट्टा वा गलत विवरण तथा कागजात दाखिला गरेको देखिएमा,

(ग) प्रमाणीकरण निकायले सार्वजनिक हित वा राष्ट्रिय अर्थतन्त्रलाई प्रतिकूल असर पर्ने किसिमबाट कारोबार सञ्चालन गरेमा,

(घ) प्रमाणीकरण निकायले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम अन्तर्गत कसूर ठहरिने कुनै काम गरेमा,

(ङ) यस ऐन बमोजिम नियन्त्रकले दिएको निर्देशनको उल्लङ्घन गरेमा।

(२) उपदफा (१) बमोजिम नियन्त्रकले इजाजतपत्र रद्द गर्नु अघि प्रमाणीकरण निकायलाई सफाई पेश गर्ने मनासिब मौका दिनु पर्नेछ।

(३) इजाजतपत्र रद्द गर्ने सम्बन्धी अन्य कार्यविधि तोकिए बमोजिम हुनेछ।

32. **<u>निर्णयको जानकारी दिनुपर्ने</u>**: (१) नियन्त्रकले दफा ३० वा ३१ बमोजिम कुनै प्रमाणीकरण निकायको इजाजतपत्र निलम्बन वा रद्द गर्ने गरी गरेको निर्णयको जानकारी त्यस्तो प्रमाणीकरण निकायलाई लिखित रुपमा दिनु पर्नेछ र त्यस्तो सूचना आफ्नो कम्प्युटर तथ्याङ्क प्रणालीमा राखी विद्युतीय स्वरुपमा समेत प्रकाशन गर्नु पर्नेछ।

(२) नियन्त्रकले इजाजतपत्र निलम्बन वा रद्द गरेको निर्णयको सूचना नेपाली र अंग्रेजी भाषाका कम्तीमा दुईवटा राष्ट्रिय दैनिक पत्रिकामा प्रकाशन गर्नु पर्नेछ।

33. **<u>विदेशी प्रमाणीकरण निकायलाई मान्यता दिन सक्ने</u>**: (१) नियन्त्रकले कुनै विदेशी मुलुकको कानून बमोजिम प्रमाणपत्र जारी गर्ने इजाजतपत्र प्राप्त गरेको प्रमाणीकरण निकायलाई नेपाल सरकारको पूर्व स्वीकृति लिई नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकिए बमोजिमको शर्त पालना गर्ने गरी मान्यता दिन सक्नेछ। यसरी मान्यता प्राप्त गरेको विदेशी प्रमाणीकरण निकायले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम बमोजिम नेपालमा प्रमाणपत्र जारी गर्न सक्नेछ।

(२) उपदफा (१) बमोजिम विदेशी प्रमाणीकरण निकायलाई मान्यता दिंदा अपनाउनु पर्ने कार्यविधि तोकिए बमोजिम हुनेछ।

34. **<u>निर्देशन दिन सक्ने</u>**: (१) नियन्त्रकले प्रमाणपत्र जारी गर्ने सम्बन्धमा यो ऐन वा यस ऐन अन्तर्गत बनेको नियम बमोजिम पूरा गर्नु पर्ने दायित्व पालन गर्न लगाउन प्रमाणीकरण निकायलाई समय समयमा आवश्यक निर्देशन दिन सक्नेछ।

(२) उपदफा (१) बमोजिम दिएको निर्देशनको पालना गर्नु सम्बन्धित प्रमाणीकरण निकायको कर्तव्य हुनेछ।

35. **<u>अधिकार प्रत्यायोजन गर्न सक्ने</u>**: नियन्त्रकले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम बमोजिम आफूले गर्नु पर्ने काम गर्न आफूलाई प्राप्त अधिकारमध्ये केही अधिकार आफ्नो मातहतका कुनै अधिकृत कर्मचारीले प्रयोग गर्न पाउने गरी प्रत्यायोजन गर्न सक्नेछ।

36. **<u>जाँचबुझ गर्न सक्ने</u>**: (१) प्रमाणीकरण निकाय वा अन्य सम्बन्धित व्यक्तिबाट यो ऐन वा यस ऐन अन्तर्गत बनेका नियमको पालना नभएको भन्ने कुरामा शंका गर्नुपर्ने मनासिव कारण भएमा नियन्त्रक आफैले वा अन्य कुनै अधिकृत कर्मचारीद्वारा तत् सम्बन्धमा आवश्यक जाँचबुझ गर्न गराउन सक्नेछ।

(२)उपदफा (१) बमोजिम जाँचवुझ गर्दा यो ऐन वा यस ऐन अन्तर्गत वनेको नियमको पालना भएको नदेखिएमा नियन्त्रकले त्यस्तो प्रमाणीकरण निकाय वा व्यक्तिलाई आवश्यक निर्देशन दिन सक्नेछ।

(३) उपदफा (१) बमोजिमको जाँचबुझमा सहयोग पुर्याउनु प्रमाणीकरण निकायको कर्तव्य हुनेछ।

(४) उपदफा (१) बमोजिम गरिने जाँचबुझको सम्बन्धमा नियन्त्रक वा अन्य कुनै अधिकृत कर्मचारीले अपनाउनु पर्ने कार्यविधि तोकिए बमोजिम हुनेछ।

37. **कार्य सम्पादन परीक्षण**: (१) नियन्त्रकले प्रत्येक वर्ष प्रमाणीकरण निकायको कार्य सम्पादनको परीक्षण गर्न गराउन सक्नेछ।

(२) उपदफा (१) बमोजिमको कार्य सम्पादन परीक्षण गर्नको लागि नियन्त्रकले कम्प्युटर सुरक्षणमा विशेषज्ञता हासिल गरेका मान्यता प्राप्त लेखापरीक्षक वा कम्प्युटर विशेषज्ञलाई नियुक्त गर्न सक्नेछ।

(३) उपदफा (१) बमोजिम गरिएको कार्य सम्पादन परीक्षणको प्रतिवेदन नियन्त्रकले आफ्नो कम्प्युटर तथ्याङ्क प्रणालीमा राखी विद्युतीय स्वरुपमा प्रकाशन गर्नु पर्नेछ।

(४) कार्य सम्पादन परीक्षण गर्ने परीक्षकको योग्यता, पारिश्रमिक र परीक्षणको कार्यविधि तोकिए बमोजिम हुनेछ।

(५) नियन्त्रकले प्रमाणीकरण गर्ने निकायको सेवास्तर निर्धारण गरी सोको सूचना सर्वसाधारणको जानकारीको लागि सार्वजनिक रुपमा प्रकाशन गर्नु पर्नेछ।

38. **कम्प्युटर र तथ्याङ्कमा पहुँच पाउने**: (१) कसैले डिजिटल हस्ताक्षर सम्बन्धमा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको उल्लंघन गरेको छ भन्ने शङ्का गर्नु पर्ने कारण तत्काल प्राप्त प्रमाणबाट देखिएमा कम्प्युटर प्रणाली, उपकरण, यन्त्र, तथ्याङ्क, सूचना प्रणाली वा त्यस्तो कार्यमा प्रयोग भएको प्रणालीसँग जोडिएको कुनै पनि सामग्रीमा पहुँच पाउने अधिकार नियन्त्रकलाई हुनेछ।

(२) उपदफा (१) को प्रयोजनको लागि नियन्त्रकले कुनै पनि कम्प्युटर प्रणाली, उपकरण, यन्त्र, तथ्याङ्क, सूचना प्रणाली वा त्यस्तो सूचना प्रणालीसँग जोडिएको कुनै पनि सामग्रीको धनी वा अन्य जिम्मेवार व्यक्तिलाई निजले आवश्यक ठानेको प्राविधिक वा अन्य सहायता उपलब्ध गराउन निर्देशन दिन सक्नेछ।

(३) उपदफा (२) बमोजिम दिएको निर्देशनको पालना गर्नु सम्बन्धित व्यक्तिको कर्तव्य हुनेछ।

39. **अभिलेख राख्नु पर्ने**: (१) यस ऐन बमोजिम जारी गरिएका सम्पूर्ण प्रमाणपत्रको अभिलेख नियन्त्रकले राख्नु पर्नेछ।

(२) उपदफा (१) को प्रयोजनको लागि डिजिटल हस्ताक्षरको गोपनीयता र सुरक्षालाई सुनिश्चित गर्न नियन्त्रकले देहाय बमोजिमका कार्य गर्नेछः—

(क) कम्प्युटर सुरक्षण प्रणाली उपयोग गर्ने,

(ख) डिजिटल हस्ताक्षरको गोपनीयता र अखण्डतालाई सुनिश्चित गर्न सुरक्षण कार्यविधि लागू गर्ने,

(ग) तोकिए बमोजिमको मापदण्डको पालना गर्ने।

(३) नियन्त्रकले सबै सार्वजनिक साँचोहरुको विवरण एउटा कम्प्युटर प्रणालीमा आबद्ध कम्प्युटर तथ्याङ्क प्रणाली अद्यावधिक रुपमा कायम गरी राख्नु पर्नेछ।

(४) डिजिटल हस्ताक्षर सम्पुष्टि गर्ने प्रयोजनको लागि सार्वजनिक साँचो उपलब्ध गराउन अनुरोध गर्ने कुनै पनि व्यक्तिलाई नियन्त्रकले सार्वजनिक साँचो उपलब्ध गराउनु पर्नेछ।

40. **झुट्टा व्यहोराको सूचना दिन नहुने**: कसैले यस ऐन बमोजिम प्राप्त गर्नु पर्ने इजाजतपत्र वा प्रमाणपत्र प्राप्त गर्न नियन्त्रक वा प्रमाणिकरण निकाय समक्ष पेश गर्नुपर्ने सूचना झुट्टा व्यहोराको पेश गर्नु हुदैन।

41. **इजाजतपत्र प्राप्त नगरी काम गर्न नहुने :** कसैले यस ऐन बमोजिम नियन्त्रकले जारी गरेको इजाजतपत्र प्राप्त नगरी प्रमाणीकरण निकायको रुपमा कार्य गर्न वा गराउन हुदैन।

42. **<u>तोकिएको विवरण वा कागजात दाखिला गर्नु पर्ने:</u>** (१) यो ऐन वा यस ऐन अन्तर्गत बनेका नियम बमोजिम नियन्त्रक वा प्रमाणीकरण निकाय समक्ष कुनै विवरण, कागजात वा प्रतिवेदन दाखिला गर्नु पर्ने जिम्मेवारी भएको व्यक्तिले तोकिएको म्यादभित्र त्यस्तो विवरण, कागजात वा प्रतिवेदन दाखिला गर्नु पर्नेछ।

(२) यो ऐन वा यस ऐन अन्तर्गत बनेका नियम बमोजिम रीतपूर्वक सुरक्षितसाथ राख्नु पर्ने कुनै किताब, रजिष्टर, स्रेस्ता, लेखा आदि सुरक्षित तथा रीतपूर्वक राख्नु पर्नेछ।

43. **<u>प्रमाणपत्र जारी गर्न सक्ने</u>**: यस ऐन बमोजिम इजाजतपत्र प्राप्त गरेको प्रमाणीकरण गर्ने निकायले मात्र विद्युतीय हस्ताक्षर सम्बन्धी प्रमाणपत्र जारी गर्न सक्नेछ।

44. **<u>प्रमाणपत्रको लागि निवेदन दिनु पर्ने</u>** : (१) डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र प्राप्त गर्न चाहने व्यक्तिले तोकिए बमोजिमको ढाँचामा तोकिए बमोजिमको शुल्क तथा विवरण समेत संलग्न गरी प्रमाणीकरण निकाय समक्ष निवेदन दिनु पर्नेछ।

(२) उपदफा (१) बमोजिमको निवेदन पर्न आएमा प्रमाणीकरण निकायले तोकिए बमोजिमको कार्यविधि पूरा गरी निवेदन प्राप्त भएको एक महिना भित्र निवेदकलाई प्रमाणपत्र जारी गर्ने वा नगर्ने भन्ने सम्बन्धमा निर्णय गरिसक्नु पर्नेछ।

(३) प्रमाणीकरण निकायले उपदफा (२) बमोजिम प्रमाणपत्र जारी गर्ने निर्णय गरेमा पन्ध्र दिनभित्र आफ्नो हस्ताक्षर सहित तोकिए बमोजिमको ढाँचामा तोकिए बमोजिमको विवरण समावेश भएको प्रमाणपत्र जारी गर्नु पर्नेछ र प्रमाणपत्र जारी नगर्ने निर्णय गरेमा सोको कारण सहितको सूचना पन्ध्र दिनभित्र निवेदकलाई दिनु पर्नेछ।

45. **<u>प्रमाणपत्र निलम्बन गर्न सक्ने</u>**: (१) प्रमाणीकरण निकायले देहायका अवस्थामा प्रमाणपत्र निलम्बन गर्न सक्नेछः—

(क) सार्वजनिक हित विपरीत हुने अवस्थामा प्रमाणपत्रलाई निलम्बन गर्न आवश्यक भएमा,

(ख) प्रमाणपत्र प्राप्त व्यक्तिले यो ऐन वा यस ऐन अन्तर्गत बनेको नियममा लेखिएको कुराको पालना नभएको कारणबाट त्यस्तो प्रमाणपत्र माथि भर पर्ने व्यक्तिहरुका लागि उल्लेखनीय हानि नोक्सानी हुनसक्ने देखिएमा सो कुराको कारण खुलाई त्यस्तो प्रमाणपत्र निलम्बन गर्न नियन्त्रकले निर्देशन दिएमा।

(२) प्रमाणपत्रको निलम्बन र निलम्बनको फुकुवा गर्ने सम्बन्धी आधार र कार्यविधि तोकिए बमोजिम हुनेछ।

46. **<u>प्रमाणपत्र रद्द गर्न सक्नेे</u>**: (१) नियन्त्रक वा प्रमाणीकरण निकायले देहायका अवस्थामा प्रमाणपत्र रद्द गर्न सक्नेछ :—

(क) प्रमाणपत्र प्राप्त गर्ने प्रयोगकर्ता वा त्यस्तो प्रयोगकर्ताको तर्फबाट अख्तियारी पाएको व्यक्तिले सो प्रमाणपत्र रद्द गरी पाउनको लागि अनुरोध गरेमा,

(ख) तोकिए बमोजिम सार्वजनिक हित विपरीत हुनेे अवस्थामा प्रमाणपत्रलाई रद्द गर्न आवश्यक भएमा,

(ग) प्रयोगकर्ताको मृत्यु भएमा,

(घ) प्रयोगकर्ता कुनै कम्पनी वा सङ्गठित संस्था भए त्यस्तो सङ्गठित संस्था वा कम्पनी प्रचलित कानून बमोजिम दामासाहीमा परेमा, खारेजी वा विघटन भएमा,

(ङ) प्रमाणपत्र जारी गर्दा पूरा गर्नु पर्ने कुनै शर्त पूरा नभएको प्रमाणित भएमा,

(च) प्रमाणपत्रमा स्पष्ट पारिएको कुनै आधारभूत तथ्य झुट्टा प्रमाणित भएमा,

(छ) प्रमाणपत्रको विश्वसनीयतामा तात्विक रुपमा असर पर्ने गरी जोडी साँचो सृजना गर्न प्रयोग गरिएको साँचो वा सुरक्षण प्रणालीमा फेरबदल वा काँटछाँट गरिएमा।

(२) प्रमाणपत्र रद्द गर्दा नियन्त्रक वा प्रमाणीकरण निकायले पालना गर्नु पर्ने कार्यविधि तोकिए बमोजिम हुनेछ।

47. **<u>प्रमाणपत्र निलम्बन वा रद्द गरिएको सूचना</u>**ः (१) दफा ३० वा ३१ बमोजिम प्रमाणपत्रको निलम्बन वा रद्द गरिएकोमा त्यसरी प्रमाणपत्र रद्द गर्ने वा निलम्बन गर्ने प्रमाणीकरण निकाय वा नियन्त्रकले सोको अभिलेख राखी त्यसको सूचना सार्वजनिक रुपमा प्रकाशन गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिम निलम्बन वा रद्द गरिएको सूचना यथाशीघ्र प्रयोगकर्तालाई दिनु पर्ने दायित्व प्रमाणीकरण निकायको हुनेछ।

48. **<u>झुट्टा प्रमाणपत्र पेश गर्न नहुने :</u>** कसैले प्रमाणपत्रमा उल्लेख भएको प्रमाणीकरण निकायले सो प्रमाणपत्र जारी गरेको होइन वा सो प्रमाणपत्रमा सूचीकृत गरिएको ग्राहकले सो प्रमाणपत्र स्वीकार गरेको छैन वा सो प्रमाणपत्र निलम्बन वा रद्द भइसकेको छ भन्ने जानि–जानि त्यस्तो प्रमाणपत्रको प्रकाशन गरेमा वा अन्य कसैलाई कुनै व्यहोराले उपलब्ध गर्न वा गराउन हुँदैन।

तर निलम्बन वा रद्द भइसकेको प्रमाणपत्रलाई त्यसरी रद्द वा निलम्बन हुनु अगाडि गरिएको डिजिटल हस्ताक्षरको सम्पुष्टि गर्ने प्रयोजनको लागि प्रकाशन गरिएको वा उपलब्ध गराइएकोमा यस उपदफा बमोजिमको कसूर गरेको मानिने छैन।

परिच्छेद-४

<u>प्रयोगकर्ताको काम, कर्तव्य र अधिकार</u>

49. **<u>जोडी साँचो सृजना गर्ने</u>**ः (१) प्रमाणीकरण निकायबाट जारी गरिएको र प्रयोगकर्ताद्वारा स्वीकार गरिएको प्रमाणपत्रमा सूचीकृत गरिनु पर्ने सार्वजनिक साँचो समावेश भएको जोडी साँचो प्रयोगकर्ताले नै सृजना गर्नु पर्ने भएमा प्रयोगकर्ताले त्यस्तो जोडी साँचो सृजना गर्दा तोकिए बमोजिमको प्रविधि र प्रणाली प्रयोग गर्नु पर्नेछ।

(२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि जोडी साँचो सृजना गर्न प्रयोग गर्नु पर्ने सुरक्षण प्रणालीको सम्बन्धमा प्रयोगकर्ता र प्रमाणीकरण निकायका बीचमा कुनै सम्झौता भएको वा प्रमाणीकरण निकायले कुनै खास प्रणालीलाई स्वीकृत गरेको अवस्थामा त्यसरी सम्झौता भएको वा स्वीकृत गरेको सुरक्षण प्रणाली प्रयोग गर्नु प्रयोगकर्ताको कर्तव्य हुनेछ।

50. **<u>प्रमाणपत्र स्वीकार गर्ने</u>** : (१) देहायका अवस्थामा प्रयोगकर्ताले प्रमाणपत्र स्वीकार गरेको मानिनेछः-

(क) निजले सो प्रमाणपत्र प्रकाशन गरेमा वा प्रकाशनको लागि एक वा एकभन्दा बढी व्यक्तिलाई अख्तियारी प्रदान गरेमा,

(ख) निजले सो प्रमाणपत्रलाई स्वीकार गरेको छ भनी विश्वास गर्न सकिने कुनै आधार भएमा।

(२) उपदफा (१) बमोजिम प्रमाणपत्रलाई स्वीकार गरेको भएमा सो कारणबाट प्रयोगकर्ताले सो प्रमाणपत्रमा उल्लेख भएको कुनै सूचना माथि भर पर्ने व्यक्तिलाई देहायका कुराहरुको प्रत्याभूति गरेको मानिनेछः-

(क) प्रयोगकर्ताले प्रमाणपत्रमा सूचीकृत गरिएको सार्वजनिक साँचोसँग सङ्गति (एसोसियट) राख्ने निजी साँचो धारण गर्ने अख्तियारी पाएको,

(ख) प्रमाणपत्र जारी गर्ने सिलसिलामा प्रयोगकर्ताले प्रमाणीकरण निकायलाई उपलब्ध गराएको सम्पूर्ण सूचना तथा जानकारी सही र दुरुस्त भएको तथा प्रमाणपत्रमा समाविष्ट भएका सूचनासँग सम्बद्ध सबै तथ्यहरु सत्य भएको, र

(ग) प्रयोगकर्तालाई जानकारी भएसम्म वा निजले जानेबुझेसम्म प्रमाणपत्रमा उल्लेख भएका सूचना सत्य र दुरुस्त भएको।

51. **<u>निजी साँचोलाई सुरक्षित राख्नु पर्ने</u>**ः (१) प्रत्येक प्रयोगकर्ताले आफूले प्राप्त गरेको प्रमाणपत्रमा सूचीकृत गरिएको सार्वजनिक साँचोसँग सम्बन्धित निजी साँचोलाई सुरक्षित राख्न आवश्यक उपाय अवलम्बन गर्नु पर्नेछ र डिजिटल हस्ताक्षर सृजना गर्ने अख्तियारी नपाएको कुनै पनि व्यक्तिलाई त्यस्तो साँचो बारे जानकारी हुन दिनबाट रोक्न आवश्यक सबै उपायहरु अवलम्बन गर्नु पर्नेछ।

(२) प्रयोगकर्ताको निजी साँचो बारे कुनै कारणबाट कतै जानकारी गराएको भएमा वा सो साँचोमा कुनै काँटछाँट हुन गएमा प्रयोगकर्ताले सोको सूचना यथाशीघ्र प्रमाणीकरण निकायलाई दिनु पर्नेछ र त्यस्तो सूचना प्राप्त हुन आएमा प्रमाणीकरण निकायले यथाशिघ्र प्रमाणपत्र निलम्बन गर्नु पर्नेछ।

(३) यस ऐन बमोजिम प्रमाणपत्र निलम्बन भएमा त्यस्तो निलम्बन अवधिभर यो दफा बमोजिम निजी साँचो सुरक्षित राख्नु प्रयोगकर्ताको कर्तव्य हुनेछ।

52. **<u>निजी साँचो नियन्त्रक समक्ष दाखिला गर्नु पर्ने</u>**ः (१) नेपालको सार्वभौमिकता वा अखण्डताको रक्षा गर्न वा मित्रराष्ट्रहरुसँगको मैत्रीपूर्ण सम्बन्धलाई कायम राख्न, शान्ति सुरक्षा कायम राख्न, प्रचलित कानून बमोजिम कसूर ठहर्ने कुनै कार्य हुनबाट रोक्न वा तोकिए बमोजिमको अन्य अवस्थामा नियन्त्रकले कुनै प्रयोगकर्तालाई कारण खुलाई निजी साँचो आफू समक्ष दाखिला गर्न आवश्यक ठानी निर्देशन दिएमा त्यस्तो प्रयोगकर्ताले सो निजी साँचो तुरुन्त नियन्त्रक समक्ष दाखिला गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिमको निर्देशन उपर चित्त नबुझेमा निजि साँचो बुझाएको पैतिस दिन भित्र सम्बन्धित व्यक्तिले सूचना प्रविधि न्यायाधिकरणमा पुनरावेदन गर्न सक्नेछ।

(३) उपदफा (१) बमोजिम दाखिला भएको निजी साँचो बारे नियन्त्रकले अनधिकृत व्यक्तिलाई जानकारी गराउन हुँदैन।

53. **पहिचानको दुरुपयोग गर्न नहुने:** कसैले विद्युतीय माध्यममा रहेको व्यक्ति तथा संस्थाको निजि साँचो, पासवर्ड वा अन्य विद्युतीय स्वरुपमा रहेको पहिचानको स्थानान्तरण, नियन्त्रण वा प्रयोग विद्युतीय प्रणालीको उपयोग गरी प्रचलित कानूनले अपराधको रुपमा तोकेको कार्य गर्ने मनसायले कुनै कार्य गर्न वा कुनै गैरकानूनी कार्यमा पहिचान दुरुपयोग गर्नु हुदैन।

54. **विद्युतीय प्रणालीमा अवरोध गर्न नहुने** : कसैले दुराशय राखी कुनै विद्युतीय प्रणालीको कार्य सञ्चालनमा बाधा पुऱ्याउन वा कार्य गर्न नसक्ने/असक्षम बनाउन वा हस्तक्षेप गर्न वा विद्युतीय प्रणालीको सञ्चालनकर्ता वा प्रयोगकर्तालाई प्रणालीको सञ्चालन वा प्रयोगमा बाधा पुर्याउन, रोक लगाउन वा हस्तक्षेप गर्न हुदैन।

परिच्छेद-५

विद्युतीय माध्यमबाट सेवा प्रवाह सम्बन्धी व्यवस्था

55. **सार्वजनिक सेवा प्रदान गर्न सकिने** : (१) सरकारी निकाय तथा सार्वजनिक संस्थाले आफूले प्रदान गर्ने सार्वजनिक सेवाहरु तोकिएको प्रकृया पूरा गरी विद्युतीय माध्यमबाट उपलब्ध गराउन सक्नेछन्।

(२) नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकेका सार्वजनिक सेवाहरू सम्बन्धित निकायले तोकिएको समयावधि भित्र विद्युतीय माध्यमबाट उपलब्ध गराउनु पर्नेछ।

(३) प्रदेश सरकार तथा स्थानीय तहले प्रदान गर्ने सार्वजनिक सेवाहरु विद्युतीय माध्यमको प्रयोग गरी वेबपोर्टल मार्फत प्रदान गर्न सक्नेछन्।

(४) उपदफा (२) र (३) बमोजिमका सेवाहरू नेपाल सरकारको केन्द्रीय वेबपोर्टल मार्फत एकिकृत रुपमा प्रदान गर्न मिल्ने गरी व्यवस्था गर्नु पर्नेछ।

(५) उपदफा (२) र (३) बमोजिमका सेवाहरू प्रवाह गर्दा सेवाग्राहीले एउटै विवरण विभिन्न निकायहरुमा पटक पटक पेश गर्नु पर्ने अवस्थाको अन्त्य गर्ने गरी राष्ट्रिय परिचयपत्रलाई विद्युतीय पहिचान (ई-केवाइसी) को रुपमा विकास गर्नु पर्नेछ।

(६) यस दफा बमोजिमका सार्वजनिक सेवा तोकिएको विद्युतीय पहिचानको आधारमा उपलब्ध गराउनु पर्नेछ।

56. **विद्युतीय माध्यमबाट सेवा प्राप्त गर्ने:** (१) सेवाग्राहीले सरकारी निकाय वा सार्वजनिक संस्थाबाट प्रदान गरिने सेवा प्राप्त गर्नका लागि सम्बन्धित सरकारी निकाय तथा सार्वजनिक संस्थामा विद्युतीय माध्यमबाट निवेदन दिन सक्नेछन्।

(२) उपदफा (१) बमोजिमको निवेदनसाथ संलग्न गर्नु पर्ने कागजात तथा अन्य विवरण तोकिए बमोजिम हुनेछ।

(३) उपदफा (१) बमोजिम प्राप्त निवेदन उपर सरकारी निकाय वा सार्वजनिक संस्थाले आवश्यक जाँचबुझ गरी माग बमोजिमको सेवा उपलब्ध गराउनु पर्नेछ।

(४) यस दफा बमोजिम उपलब्ध गराइने सेवा सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

57. <u>सूचना तथा तथ्याङ्क विद्युतीय स्वरूपमा राख्नु पर्ने</u> : (१) सरकारी निकाय वा सार्वजनिक संस्थाले आफूले सिर्जना, संकलन तथा प्राप्त गरेका सूचना विद्युतीय स्वरुपमा राख्नुपर्नेछ।

(२) उपदफा (१) बमोजिमको सूचना विद्युतीय स्वरुपमा राख्दा तोकिए बमोजिमको सुरक्षा तथा गोपनीयता सम्बन्धी मापदण्ड पुरा गर्नु पर्नेछ।

(३) उपदफा (१) बमोजिमका सूचना समयबद्धरुपमा पुनः प्रयोग गर्न मिल्ने गरी अभिलेखिकरण गर्नु पर्नेछ।

58. <u>विद्युतीय स्वरुपमा प्रकाशन, अभिलेखीकरण तथा कारोबार गर्नुपर्ने</u>: (१) नेपाल सरकारले प्रचलित कानून बमोजिम नेपाल राजपत्रमा प्रकाशन गर्नु पर्ने अध्यादेश, ऐन, नियम, गठन आदेश, सूचना वा अन्य विषयलाई विद्युतीय स्वरुपमा प्रकाशन गर्नु पर्नेछ।

(२) सरकारी निकाय वा सार्वजनिक संस्था वा नेपालभित्र कारोबार गर्ने बैङ्क वा वित्तीय संस्थामा प्रचलित कानून बमोजिम राख्नु पर्ने अभिलेख तथा गरिने कारोबार विद्युतीय स्वरुप वा विद्युतीय सञ्चार माध्यमको प्रयोगबाट गर्नु पर्नेछ।

(३) सरकारी वा सार्वजनिक संस्था वा कुनै व्यक्तिले कुनै किसिमको वस्तु वा सेवा खरिद तथा बिक्री गरेमा विद्युतीय माध्यमको प्रयोग गरी भुक्तानी गर्नु पर्नेछ।

(४) उपदफा (३) बमोजिमको भुक्तानी सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

(५) उपदफा (१), (२) र (३) बमोजिम विद्युतीय स्वरुप वा विद्युतीय सञ्चारमाध्यमको प्रयोग गरी भएको विद्युतीय प्रकाशन, अभिलेखिकरण, कारोवार तथा भुक्तानीले कानूनी मान्यता प्राप्त गर्नेछ।

59. <u>सूचना प्रविधि प्रणाली प्रयोग गर्नुपर्ने</u>: (१) सरकारी निकायले विभागको सिफारिसमा मन्त्रालयले स्वीकृत गरेको मापदण्ड बमोजिमको सूचना प्रविधि प्रणालीको प्रयोग गर्नु पर्नेछ।

(२) सरकारी निकायले सूचना प्रविधि प्रणाली मार्फत सूचना खुला मानक (ओपन स्टयाण्डर्ड)मा संरक्षण गरी राख्नु पर्नेछ।

(३) उपदफा (१) बमोजिमको सूचना प्रविधि प्रणालीको सूचनामा सम्बन्धित सरकारी निकायको स्वामित्व हुनु पर्नेछ।

(४) उपदफा (१) बमोजिमको सूचना प्रविधि प्रणालीले सरकारी निकायका सूचना प्रविधि प्रणाली बीच अन्तरआवद्धता गरी तथ्यांक एवं सूचना आदानप्रदान गर्नु पर्नेछ।

(५) सरकारी निकायले सूचना प्रविधि प्रणाली सञ्चालन गर्नु पूर्व उपदफा (१) बमोजिमको मापदण्ड अनुरुप भए नभएको परीक्षण तोकिए बमोजिम विभागबाट गराउनु पर्नेछ।

(६) उपदफा (१) बमोजिमको मापदण्ड अनुसार प्रणालीको प्रयोग नगरेमा विभागको सिफारिसमा मन्त्रालयले सम्बन्धित सरकारी निकायको प्रशासकीय प्रमुखलाई प्रचलित कानून बमोजिम विभागीय कारबाहीको लागि लेखि पठाउन सक्नेछ।

(७) उपदफा (१) बमोजिमको मापदण्ड प्रयोग गर्ने सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

60. **डिजिटल हस्ताक्षर प्रयोग गर्न सक्ने**ः सरकारी निकाय र सार्वजनिक संस्थाले यस ऐन बमोजिमको डिजिटल हस्ताक्षर प्रयोग गर्न सक्नेछन्।

61. **वेबसाइट सञ्चालनमा ल्याउनुपर्ने** :(१) प्रत्येक सरकारी निकाय र सार्वजनिक संस्थाले सूचना प्रवाह तथा सेवा प्रदान गर्न आफ्नो वेबसाइट सञ्चालन गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिम सञ्चालन हुने वेवसाइटको विकास र सुरक्षित सञ्चालन सम्बन्धी न्यूनतम मापदण्ड तथा सञ्चालन विधि मन्त्रालयले तोके बमोजिम हुनेछ।

62. **सूचना प्रविधि प्रणालीको विकासमा संलग्नता हुनुपर्ने** : (१) सरकारी निकायले सूचना प्रविधि प्रणाली सम्बन्धी विकासमा नेपाल सरकारको सूचना प्रविधि सम्बन्धी अधिकृत स्तरको कर्मचारीको संलग्नतामा गराउनु पर्नेछ।

(२) सार्वजनिक निकायको लागि विकसित सूचना प्रविधि प्रणालीको सफ्टवेयर कोड सहितको सम्पूर्ण संरचनाको पूर्ण स्वामित्व सम्बन्धित सार्वजनिक निकायको हुनेछ।

63. **सूचना प्रविधि सम्वन्धी प्राविधिक परीक्षण गर्ने गराउने:** (१) नेपाल सरकारले सरकारी निकायमा प्रयोगमा रहेका सूचना प्रविधि प्रणाली, पूर्वाधार र कार्य प्रणालीको आन्तरिक प्राविधिक परीक्षण गर्नका लागि छुट्टै कार्यालयको स्थापना गर्न सक्नेछ।

(२) कार्यालयको काम कर्तव्य र अधिकार देहाय वमोजिम रहनेछ:

(क) सूचना प्रविधि सम्बन्धी कार्य कानून बमोजिम भए नभएको बारे अध्ययन गरी प्रतिवेदन पेश गर्ने,

(ख) सूचना प्रविधि प्रणाली र पूर्वाधार संचालनको प्राविधिक परिक्षण गर्ने,

(ग) सूचना प्रविधि सम्बन्धी कानुनी,व्यवहारगत,कार्यगत प्रावधान एवं मापदण्डका सम्बन्धमा गर्नुपर्ने सुधारका सम्बन्धमा अध्ययन गरी आवश्यक सिफारिस गर्ने।

64. **भेटिङ्ग सम्वन्धी व्यवस्था:** (१) भेटिङ्ग सम्वन्धी कार्य विभागले गर्नेछ।

स्पष्टीकरण: यस दफाको प्रयोजनको लागि "भेटिङ्ग" भन्नाले सरकारी निकायको सूचना प्रविधि प्रणालीको आवश्यकता र उपयोगिताको सुनिश्चित गर्न, वास्तविक र सुरक्षित प्रयोगको प्रत्याभूत गर्न, परमार्शदाता एवं निर्माणकर्ताको क्षमताको सुनिश्चित गर्न, सफ्टवेयर तथा हार्डवेयरको पूर्णताको जाँच गर्न, सफ्टवेयरको दोहोरोपना, सुरक्षा कमजोरी र सोसँग सम्बन्धित मापदण्ड, ऐन, नियमको पालना सम्बन्धमा जाँच गरी सम्भावित जोखिम न्यूनीकरण गर्ने कार्यलाई सम्झनु पर्छ।

(२) उपदफा (१) बमोजिम विभागले भेटिङ्ग सञ्चालन गर्न सो सम्बन्धी मापदण्ड तयार गर्ने, आवश्यक प्रणाली बिकास गर्ने, कम्पनीको जाँच प्रक्रिया सहज गराउने, सेवा वर्गीकरण गर्ने गराउनेछ।

(३) सार्वजनिक निकायसँग आवद्ध भई प्रणाली विकास तथा बिक्री गर्ने निजी तथा सार्वजनिक निकायहरूले उपदफा (२) बमोजिम तोकिएको मापदण्ड पूरा गरी तोकेको सेवा वर्गीकरण बमोजिम विभागमा सूचीकृत हुनु पर्नेछ।

(४) सार्वजनिक निकायले सफ्टवेयर एवं हार्डवेयर प्रणाली विभागबाट भेटिङ्ग गराई खरिद तथा प्रयोग गर्नु पर्नेछ।

(५) यो ऐन लागु हुनुभन्दा अगाडि प्रयोगमा रहेका सफ्टवेयर तथा हार्डवेयर प्रणाली यो ऐन लागु भएको एक वर्ष भित्र विभागबाट भेटिङ्ग गराउनु पर्नेछ।

(६) उपदफा (५) बमोजिम तोकिएको अवधि भित्र विभागबाट भेटिङ्ग नगराई कसैले सफ्टवेयर तथा हार्डवेयर प्रणाली प्रयोगमा गरेको पाइएमा विभागले जुनसुकै समयमा बन्द गर्न, गराउन सक्नेछ।

(७) भेटिङ्ग सञ्चालन सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

65. **पृष्ठपोषण लिन सक्ने**: (१) नेपाल सरकारले कानून तर्जुमा वा नीति निर्माण गर्दा आवश्यकता अनुसार विद्युतीय माध्यमबाट सर्वसाधारणको पृष्ठपोषण लिन सक्नेछ।

(२) प्रदेश सरकार तथा स्थानीय तहले कुनै निर्णय वा कानून निर्माण गर्ने प्रक्रियामा सर्वसाधारणको पृष्ठपोषण लिन आवश्यक ठानेमा विद्युतीय माध्यमबाट लिन सक्नेछन्।

परिच्छेद-६

डोमेन नाम दर्ता तथा व्यवस्थापन

66. **डोमेन नाम सेवा सञ्चालन, नियमन तथा व्यवस्थापन:** (१) डोमेन नाम, सेवाको नियमन तथा व्यवस्थापन विभागले गर्नेछ।

67. **डोमेन नाम दर्ता गर्नु पर्ने**: (१) कुनै व्यक्ति वा संस्थाले एनपी डोमेनमा नाम दर्ता गराउँदा विभागले तोकेको संस्थामा तोकिए बमोजिमको दस्तुर बुझाई दर्ता गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिम दर्ता भएको डोमेन नाम अरु कसैले प्रयोग गर्न पाउने छैन।

(३) उपदफा (१) बमोजिम दर्ता भएका डोमेन नामसँग झुक्किने किसिमले मिल्दोजुल्दो हुने गरी डोमेन नाम दर्ता गर्न वा गराउन हुँदैन।

(४) सरकारी निकायले आफ्नो कार्यालयको डोमेन नाम गभर्मेन्ट डट एनपी अन्तर्गत दर्ता गर्नुपर्नेछ।

(५) उपदफा (१) बमोजिम दर्ता भएको डोमेन नाम प्रत्येक दुई वर्षमा तोकिए बमोजिमको दस्तुर बुझाई नविकरण गर्नु पर्नेछ।

(६) यो ऐन जारी हुँदाका वखत सञ्चालनमा रहेका डोमेन नामहरु यो ऐन प्रारम्भ भएको मितिले छ महिनाभित्र यस ऐन बमोजिम दर्ता गर्नु पर्नेछ।

(७) डोमेन नाम सञ्चालन सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

68. **डोमेन नाम सुरक्षित रहने :** (१) देहाय बमोजिमका नाम दोश्रो र तेश्रो तहका डोमेन नामको लागि सुरक्षित रहनेछन्:—

(क) प्रचलित कानून बमोजिम कुनै कम्पनीको नाममा दर्ता गरिएको ट्रेडनाम,

(ख) भौगोलिक तथा पर्यटकीय स्थलहरुको नाम,

(ग) पुरातत्विक तथा धार्मिक महत्वका नाम,

(घ) राष्ट्रियरुपमा ख्याति प्राप्त व्यक्तिका नाम,

(ङ) सरकारी संस्थाहरुको नाम,

(च) अन्तराष्ट्रिय गैर सरकारी संस्थाहरुको नाम,

(छ) नेपाल सरकारले तोकेका अन्य नाम।

(२) उपदफा (१) बमोजिमका डोमेन नामहरु खण्ड (क), (घ) र (ङ) बमोजिमका नामहरू सम्बन्धित संस्थाको प्रयोगमा मात्र र अन्यको हकमा नेपाल सरकारले तोकेको निकायको स्वीकृति लिई प्रयोग गर्न पाईनेछ।

(३) उपदफा (१) बमोजिमका सुरक्षित नामहरुसँग बाझिने गरि मिल्दोजुल्दो वा उक्त नामको महत्वलाई अवमुल्यन गर्ने गरि डोमेन नाम दर्ता गर्न वा गराउन हुँदैन।

69. **अन्य भाषामा डोमेन नामको प्रयोग**: यस परिच्छेदमा अन्यत्र जुनसुकै कुरा लेखिएको भए तापनि कुनै राष्ट्र भाषामा डोमेन नाम दर्ता तथा प्रयोग गर्न बाधा पुगेको मानिने छैन।

70. **आवश्यक निर्देशन दिन सक्ने:** डोमेन नामको सञ्चालनलाई भरपर्दो र सुरक्षित बनाउनको लागि विभागले डोमेन नाम प्रणाली सञ्चालकलाई आवश्यक निर्देशन दिन सक्नेछ।

71. **अनाधिकृत रुपमा डोमेन नाम प्रणाली सञ्चालन गर्न नहुने**: कसैले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम विपरीत अनाधिकृत रुपले डोमेन नाम प्रणाली सञ्चालन गर्न वा गराउन हुँदैन।

परिच्छेद-७

सूचना प्रविधि सम्बन्धी उद्योग र व्यवसाय सम्बन्धी व्यवस्था

72. **सूचना प्रविधि सम्बन्धी उद्योग वा व्यवसायको दर्ताको जानकारी:** सूचना प्रविधि सम्बन्धी उद्योग वा व्यवसायको सञ्चालन गर्नुअघि विभागको स्वीकृति अनिवार्य लिनुपर्नेछ र दर्ता तथा खारेज पश्चात सोको जानकारी विभागलाई दिनु पर्नेछ।

73. **स्वीकृत मापदण्डका उपकरण मात्र पैठारी एवं बिक्री वितरण गर्नु पर्ने:** (१) सूचना प्रविधि सम्बन्धी तोकिए बमोजिमका उपकरणको हकमा मन्त्रालयले स्वीकृत गरेको मापदण्डको आधारमा मात्र पैठारी एवं बिक्री वितरण गर्न पाइनेछ।

(२) उपदफा (१) बमोजिमको मापदण्ड, उपकरणहरुको गुणस्तर, आयु र सुरक्षाको आधारमा स्वीकृत गर्ने प्रकृया र ई-वेष्ट व्यवस्थापन सम्बन्धी अन्य व्यबस्था तोकिए बमोजिम हुनेछ।

74. **अनुमति नलिई उपकरणको प्रयोग गर्न नहुने**: कसैले दफा ७३ को उपदफा (१) बमोजिमका उपकरणहरुको अनुमति नलिई वा अनुमति लिएको अवधि भन्दा वढी अवधि प्रयोग गर्न वा अरु कसैलाई प्रयोगको लागि उपलब्ध गराउन हुँदैन।

75. **सूचना प्रविधि सम्बन्धी उद्योगको प्रवर्द्धन गर्नुपर्ने :** (१) नेपालमा दर्ता भई सञ्चालनमा रहेका सूचना प्रविधि सम्बन्धी उद्योगहरुलाई नेपाल सरकारले प्रवर्द्धन र सहजीकरण गर्नु पर्नेछ।

(२) सूचना प्रविधिसँग सम्बन्धी बहुराष्ट्रिय संस्था वा कम्पनीहरुलाई नेपालमा व्यवसाय सञ्चालन गर्न नेपाल सरकारले सहजीकरण गर्नुपर्नेछ।

(३) यस सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

76. **आउटसोर्सिङ मार्फत उद्योग व्यवसाय सञ्चालन गर्न सकिने**: (१) कुनै पनि व्यक्ति वा संस्थाले आउटसोर्सिङ गरी उद्योग व्यवसाय सञ्चालनको लागि अनिवार्यरुपमा प्रचलित कानून बमोजिम दर्ता गर्नुपर्नेछ।

(२) उपदफा (१) बमोजिमको दर्ताको लागि विभागको सिफारिस अनिवार्य रुपमा लिनुपर्नेछ।

(३) आउटसोर्सिङ सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

77. **नेपालमा उत्पादित सूचना प्रविधि प्रणालीको प्रयोग**: (१) नेपालको आफ्नै अनुसन्धानमा आधारित सूचना प्रविधि प्रणाली विकासमा जोड दिनुपर्नेछ।

(२) नेपालमा उत्पादित सूचना प्रविधि प्रणालीको प्रयोगलाई प्राथमिकता दिनु पर्नेछ।

78. **नवीनतम प्रविधिको प्रयोग**: (१) सूचना तथा सञ्चार प्रविधिको क्षेत्रमा विकसित भएका आर्टिफिसियल इन्टेलिजेन्स, मेसिन लर्निङ्ग, वल्कचेन, आइ.ओ.टी. लगायतका नवीनतम प्रविधिको मर्यादित,पारदर्शी,जवाफदेही र सुरक्षित प्रयोग गर्नुपर्नेछ।

(२) उपदफा (१) मा उल्लेखित प्रविधिको उपयोग, प्रवर्धन र विस्तार सरकारी, सार्वजनिक र निजी क्षेत्रमा समेत गर्नुपर्नेछ।

(३) उपदफा (१) मा उल्लेखित प्रविधिको व्यवस्थित प्रयोगको समन्वय र सहजीकरण विभागले गर्नेछ। यसको अनुसन्धान र विकासको लागि नेपाल सरकारले सेन्टर फर एक्सलेन्सको व्यवस्था गर्नुपर्नेछ।

(४) यस सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

परिच्छेद-८

सूचना सुरक्षा तथा गोपनियता सम्बन्धी व्यवस्था

79. **सूचना सुरक्षा सम्बन्धी व्यवस्था:** (१) कसैले विद्युतीय प्रणालीको प्रयोग गरी नेपालको राष्ट्रिय सुरक्षा, सार्वभौमसत्ता, भौगोलिक अखण्डता, राष्ट्रियता वा राष्ट्रिय एकता, स्वाधीनता, स्वाभिमान वा सःघीय इकाईबिचको सुसम्बन्ध खलल पार्ने वा मुलुकको सुरक्षा वा तथ्यांक प्रणालीमा अवरोध सिर्जना गर्ने वा प्रतिकूल असर पार्ने कुनै कार्य गर्न वा गराउन हुदैन।

(२) कसैले पनि विद्युतीय प्रणाली मार्फत कसैलाई प्रचलित कानून बमोजिम यौनजन्य दुर्व्यवहार मानिने कुनै कार्य गर्न वा सोको लागि कसैलाई अनुचित प्रलोभनमा पार्ने वा धम्की दिने जस्ता कुनै कार्य गर्न वा गराउन हुँदैन।

(३) कसैले विद्युतीय प्रणालीको माध्यमबाट कुनै अश्लिल सामग्रीको उत्पादन गर्न, संकलन गर्न, उपलव्ध रहेको जानकारी संप्रेषण गर्न, देखाउन, वितरण गर्न, प्रकाशन गर्न, प्रदर्शन गर्न, प्रसार गर्न वा विक्री गर्न वा संचय गर्न हुदैन।

तर कुनै व्यक्तिले कुनै अनुसन्धान, कानुन कार्यान्वयन, अध्यापन वा चिकित्सकीय प्रयोजनको लागि अश्लिल सामग्रीको संप्रेषण, प्राप्ति, वा संचय गरेको यथोचित रुपमा पुष्टि गरेमा र त्यस्तो उद्देश्य पूरा हुनासाथ त्यस्ता सामग्री मेटाएमा यस दफा बमोजिमको कसूर मानिने छैन।

(४) कसैले विद्युतीय प्रणालीको माध्यमबाट वा सो प्रणालीको उपयोग गरेर कसैलाई यौन शोषण गर्ने वा ठगी गर्ने वा अरु कुनै गैरकानूनी कार्य गर्ने मनसाय राखी कुनै प्रस्ताव राख्न, प्रलोभन पार्न, भेट्न, वा कुनै गैरकानूनी गतिविधिमा लाग्न उक्साउन वा सो को लागि अनलाईन सम्बन्ध स्थापित गर्न प्रस्ताव गर्न हुदैन।

(५) यस सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

80. **वैयक्तिक विवरणको संकलन गर्न नहुने:** (१) प्रचलित कानून बमोजिम बाहेक कसैले पनि विद्युतीय स्वरुपमा रहेको कसैको वैयक्तिक विवरण संकलन गर्न हुँदैन।

(२) कसैको वैयक्तिक विवरण संकलन गर्नु परेमा सो विवरण कुन प्रयोजनको लागि आवश्यक परेको हो सोको जानकारी सम्बन्धित व्यक्तिलाई अनिवार्य रुपमा गराउनु पर्नेछ।

(३) सूचना प्रविधि प्रणालीमा रहेका कुनै व्यक्तिको वैयक्तिक विवरण संकलन गर्दा खुलाईएको प्रयोजन बाहेक अन्य प्रयोजनका लागि प्रयोग, प्रसार तथा आदान प्रदान गर्न पाईने छैन।

तर सम्बन्धित व्यक्तिको स्वीकृतिमा वा प्रचलित कानून बमोजिम अन्य प्रयोजनका लागि प्रयोग, प्रसार तथा आदान प्रदान गर्न बाधा पर्ने छैन।

(४) कुनै खास प्रयोजनका लागि कानून बमोजिम संकलन तथा सञ्चय गरिएको वैयक्तिक सूचना संकलन तथा सञ्चयको प्रयोजन समाप्त भएको पैंतिस दिनभित्र सम्बन्धित व्यक्तिलाई प्रत्याभूत हुने गरी नष्ट गरिसक्नु पर्नेछ।

81. **सूचना सुरक्षाको प्रत्याभूत गर्नु पर्नेः** (१) विद्युतीय स्वरुपमा रहेका सूचनाको आदान प्रदान, प्रशोधन तथा सञ्चय गर्दा प्रशोधनकर्ता, सञ्चयकर्ता र सेवा प्रदायकले गोपनियता र अक्षुण्ता कायम रहने गरी गर्नु पर्नेछ।

(२) सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्य सम्बन्धी सेवा प्रदायक संस्थाहरुले तोकिएको विवरण अनिवार्य रुपमा तोके अनुसार इन्क्रिप्सन गरी सुरक्षित राख्नु पर्नेछ।

(३) सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्य सम्बन्धी सेवा प्रदायक संस्थाहरुले तोकिएको विवरणहरु प्रशोधन, सम्प्रेषण तथा भण्डारण गर्दा सूचना नेपाल बाहिर नजाने गरी सुरक्षित गर्नु पर्नेछ।

(४) सूचना सुरक्षा सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

82. **सुरक्षा मापदण्ड अवलम्बन गर्नु पर्नेः** सरकारी निकायले कम्प्युटर तथा सूचना प्रणालीको प्रयोग गर्दा तोकिए बमोजिको सुरक्षा मापदण्ड अवलम्बन गर्नु पर्नेछ।

83. **सुरक्षण परीक्षण गर्नु पर्नेः** सरकारी निकाय, सार्वजनिक संस्था र वित्तीय तथा स्वास्थ्य सम्बन्धी सूचना प्रयोग गर्ने संस्थाहरुले अनिवार्य रुपमा आफूले प्रयोग गर्ने सूचना प्रविधि प्रणालीको तोकिए बमोजिमको अवधिमा सुरक्षा परीक्षण गराउनु पर्नेछ।

84. **डाटा सेन्टर, क्लाउड तथा दुवै सेवा सञ्चालन तथा विपद व्यवस्थापन सम्बन्धी व्यवस्थाः** (१) नेपालभित्र डाटा सेन्टर, क्लाउड तथा दुवै सेवा सञ्चालन गर्न चाहने संस्थाले तोकिएको ढाँचामा तोकिए बमोजिमको दस्तुर बुझाई विभागमा निवेदन दिई इजाजतपत्र लिनु पर्नेछ।

तर कुनै संस्थाले आफ्नो निजी प्रयोजनको लागि मात्र सञ्चालन गर्ने डाटा सेन्टर, क्लाउड तथा दुवै सेवा को लागि इजाजतपत्र लिनु पर्ने छैन।

(२) उपदफा (१) बमोजिम इजाजत प्रदान गर्दा विभागले डाटा सेन्टर, क्लाउड तथा दुवै सेवा प्रदायकले तोकिए बमोजिमको मापदण्ड पूरा गरे नगरेको परीक्षण गर्नु पर्नेछ।

(३) उपदफा (१) बमोजिम इजाजतपत्र प्राप्त संस्थाले वार्षिक रुपमा अद्यावधिक विवरण विभागमा पेश गर्नुपर्नेछ। विभागले वर्षको कम्तीमा दुई पटक अनुगमन गर्नु पर्नेछ।

(४) यो ऐन प्रारम्भ हुँदाका बखत सञ्चालनमा रहेका डाटा सेन्टर, क्लाउड तथा दुवै सेवा प्रदायकहरुले यस ऐन लागू भएको एक वर्षभित्र यस दफा बमोजिमको इजाजत लिनु पर्नेछ।

(५) उपदफा (१) बमोजिमको इजाजतपत्र प्रत्येक बर्ष नवीकरण गर्नु पर्नेछ।

(६) उपदफा (१) बमोजिम इजाजतपत्र प्रदान गर्ने तथा नवीकरण गर्ने सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

(७) उपदफा (१) बमोजिम इजाजतपत्र प्राप्त संस्थाले सञ्चालित प्रणालीको विपद व्यवस्थापन सम्बन्धी व्यवस्था तोकिए बमोजिम हुनेछ।

85. <u>डाटा सेन्टर वा क्लाउडमा सूचना प्रणाली राख्नु पर्नेः</u> (१) सरकारी निकायले तोकिए बाहेकका कम्प्युटर तथा सूचना प्रणाली यस ऐनको दफा ८७ बमोजिम इजाजतपत्र प्राप्त डाटा सेन्टर तथा क्लाउडमा राखी सञ्चालन गर्न सक्नेछ।

(२) डाटा सेन्टर वा क्लाउडमा कम्प्युटर प्रणालीहरु राख्ने सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

86. <u>इजाजत नलिई डाटा सेन्टर, क्लाउड वा दुवै सञ्चालन गर्न नहुनेः</u> कसैले यस ऐन बमोजिम इजाजत नलिई डाटा सेन्टर, क्लाउड वा दुवै सञ्चालन गर्न हुदैन।

87. <u>सूचना सुरक्षण अधिकृत तोक्नु पर्ने</u> (१) नेपाल सरकारको प्रत्येक मन्त्रालय, आयोग, सचिवालय र विभागमा कम्तीमा एक जना सूचना सुरक्षण अधिकृत (सूचना प्रविधि सम्बन्धी) को व्यवस्था गरी जिम्मेवारी तोक्नु पर्नेछ।

(२) उपदफा (१) बमोजिमको सूचना सुरक्षण अधिकृत सम्बन्धी योग्यता तथा अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

88. <u>विद्युतीय स्वरुपको सूचनालाई क्षति पुऱ्याउन, अवरोध गर्न नहुनेः</u> (१) कसैले दुराशय राखी वा गलत मनसाय राखी कसैको स्वामित्व वा नियन्त्रणमा रहेको विद्युतीय स्वरुपको सूचनालाई अनाधिकृत रुपमा मेटाउन, नष्ट गर्न, हेरफेर गर्न, बिगार्न, बुझ्न नसकिने गरी परिवर्तन गर्न वा अर्थहिन, प्रयोगहिन वा निष्प्रभावी गराउन हुदैन।

(२) कसैले दुराशय राखी वा गलत मनसाय राखि कसैको स्वामित्व वा नियन्त्रणमा रहेको विद्युतीय स्वरुपको सूचनाको प्रयोगलाई अनाधिकृत रुपमा बाधा पुर्याउन, रोक लगाउन वा आधिकारीक व्यक्तिलाई सूचनामा पहुँच दिन ईन्कार गर्न हुदैन।

89. <u>गोपनीयता भङ्ग गर्न नहुनेः</u> (१) कसैले पनि कानून बमोजिम वाहेक विद्युतीय माध्यमबाट कसैको वैयक्तिक विवरण वा सूचना, जानकारी, पत्राचार अनधिकृत रूपमा प्राप्त गर्न, त्यसको गोपनीयता भङ्ग गर्न वा अनधिकृत रूपमा कसैलाई उपलब्ध गराउन हुँदैन।

(२) कसैले पनि कुनै दुई वा दुईभन्दा बढी व्यक्तिहरूबीचमा विद्युतीय माध्यमबाट भएका कुनै संवाद वा कुराकानी वा संकेत सम्बन्धित व्यक्तिहरूले मञ्जुरी दिएको वा कानून बमोजिम अधिकार प्राप्त अधिकारीले आदेश दिएकोमा बाहेक कुनै यान्त्रिक उपकरणको प्रयोग गरी सुन्न वा त्यस्तो कुराको ध्वनि अङ्कन वा रेकर्ड गर्न वा गराउन हुँदैन।

तर

(१)सार्वजनिक रूपमा गरिएको भाषण वा वक्तव्यको हकमा यस उपदफाको व्यवस्था लागू हुने छैन।

(२) प्रचलित कानून बमोजिमको अवस्थामा कुनै पनि सूचना, जानकारी वा पत्राचार सुन्न, ध्वनि अङ्कन वा रेकर्ड गर्न वा गराउन सकिनेछ।

90. **<u>विद्युतीय प्रणालीको श्रोत सङ्केतको नष्ट र परिवर्तन गर्न वा चोरी गर्न नहुने:</u>** (१) कसैले विद्युतीय प्रणालीमा प्रयोग हुने श्रोत सङ्केत चोरी गर्न, अनाधिकृत रुपमा नष्ट गर्न वा परिवर्तन गर्न हुँदैन।

<u>स्पष्टीकरण:</u> यस दफाको प्रयोजनका लागि "श्रोत सङ्केत" भन्नाले कम्प्युटर कार्यक्रमहरुको सूचीकरण, कम्प्युटर निर्देशन, कम्प्युटर डिजाइन र कम्प्युटर लेआउट तथा कम्प्युटर सम्पदाको जुनसुकै स्वरुपमा रहेको कार्यक्रम विश्लेषणलाई सम्झनु पर्छ।

(२) कसैले विद्युतीय प्रणालीमा प्रयोग हुने श्रोत सङ्केत चोरीको हो भन्ने जानी जानी खरिद तथा बिक्री गर्न हुँदैन।

91. **<u>विद्युतीय प्रणालीमा रहेको सूचनाको चोरी गर्न नहुने:</u>** (१) कसैले विद्युतीय प्रणालीमा रहेको सूचना चोरी गर्न हुदैन।

(२) कसैले विद्युतीय प्रणालीमा रहेको सूचना चोरीको हो भन्ने जानी जानी खरिद तथा बिक्री गर्न हुँदैन।

92. **<u>सेवा प्रदायकले दायित्व व्यहोर्नु नपर्ने:</u>** प्रचलित कानूनमा जुनसुकै कुरा लेखिएको भए तापनि देहायको अवस्थामा सेवा प्रदायकले कुनै तेस्रो पक्षको सूचना वा तथ्याङ्क वा लिंकमा पहुँच उपलब्ध गराएको कारणबाट मात्र उक्त सूचना वा तथ्याङ्क वा लिंकमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणको सम्बन्धमा उत्पन्न हुने कुनै फौजदारी दायित्व व्यहोर्नु पर्ने छैनः-

(क) सेवा प्रदायकले सूचना, तथ्याङ्क वा लिंकमा पहुँच पुर्याउने कार्यमा मात्र सिमित रहेको भएमा,

(ख) सेवा प्रदायकले आफै प्रसारण नगरेको, प्रसारणको उपभोगकर्ता आफैं चयन नगरेको र प्रसारणमा रहेको सूचना छनौट तथा परिवर्तन नगरेको भएमा,

(ग) सेवा प्रदायकले आफ्नो सूचना प्रणालीमा भण्डारण गरेको कुनै खास सूचना गैह्रकानूनी रहेको भनी कुनै सम्बन्धित सार्वजनिक निकाय वा अदालतबाट त्यस्तो सूचना सामग्री हटाउन वा त्यस्ता सूचनामा पहुँच निष्क्रिय पार्न प्राप्त आदेश बमोजिम सेवा प्रदायकले सूचना सामग्री यथाशिघ्र हटाएमा वा पहुँच निष्क्रिय बनाएमा,

(घ) सेवा प्रदायकले नियामक निकायको सम्बन्धित निर्देशनहरु पालना गरेको भएमा।

तर कुनै सूचना, तथ्याङ्क वा लिंकमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणले प्रचलित कानूनको उल्लघंन गरेमा वा कुनै गैरकानूनी कार्य गर्न दुरुत्साहन वा सहयोग गरेमा सेवा प्रदायक त्यस्तो दायित्वबाट मुक्त हुने छैन।

93. **<u>सूचना तथा तथ्याङ्क सुरक्षित राख्नु पर्ने:</u>** सेवा प्रदायकले सेवा प्रयोग सम्बन्धी तोकिए बमोजिमका विवरणहरू तोकिएको अवधिसम्म सुरक्षित राख्नु पर्नेछ ।

परिच्छेद- ९

साइबर सुरक्षा केन्द्र सम्बन्धी व्यवस्था

94. **केन्द्रको स्थापना :** (१) साइबर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्द्धन, जनचेतना अभिवृद्धि, साइबर सुरक्षा सम्बन्धी तयारी, साइबर चुनौतीको पहिचान, रोकथाम, प्रतिक्रिया तथा पुनर्लाभ लगायतका कामको सम्पर्क निकायको रूपमा कार्य गर्न तथा डिजिटल फोरेन्सिक अनुसन्धान गर्न राष्ट्रिय साइबर सुरक्षा केन्द्र रहनेछ।

(२) केन्द्रमा संवेदनशील सूचना पूर्वाधारहरुको चौविसै घण्टा अनुगमन, साइबर घटना तथा जोखिम मूल्यांकन गर्नेछ।

(३) केन्द्रले आकस्मिक रुपमा आइपर्ने साइबर जोखिमलाई समाधान गर्नको लागि प्राविधिक जनशक्ति सहितको आकस्मिक सहायता समूहको गठन गर्नेछ।

(४) संवेदनशील सूचना पूर्वाधारको धनीले चाहेमा आफ्नै कम्प्यूटर आकस्मिक सहायता समूह बनाउन सक्नेछ। सो बमोजिमको समूह बनाउन अगाडि केन्द्रबाट पूर्व स्वीकृति लिनु पर्नेछ।

(५) आकस्मिक रुपमा आइपर्ने साइबर जोखिमलाई समाधान गर्नको लागि प्रदेश तथा स्थानीय तहले आकस्मिक सहायता समूह गठन गर्न सक्नेछन्।

(६) उपदफा (५) बमोजिम गठित समूहले केन्द्रमा गठित आकस्मिक सहायता समूहसँग समन्वय र सहकार्य गर्नुपर्नेछ।

(७) आकस्मिक सहायता समूह सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

95. **केन्द्रको काम, कर्तव्य र अधिकार:** यस ऐनमा अन्यत्र उल्लेख गरिएका काम, कर्तव्य र अधिकारको अतिरिक्त केन्द्रको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) साइबर सुरक्षा जोखिम अनुगमन गर्ने,

(ख) राष्ट्रिय सुरक्षा, प्रतिरक्षा, अर्थतन्त्र, अन्तर्राष्ट्रिय सम्बन्ध, सार्वजनिक स्वास्थ्य, सार्वजनिक शान्ति र व्यवस्था वा सार्वजनिक सुरक्षा वा अत्यावश्यक सेवालाई पार्न सक्ने साइबर सुरक्षाका घटनाको प्रतिकार्य गर्ने,

(ग) संवेदनशील सूचना पूर्वाधारहरुको पहिचान गरी निर्देशक समिति समक्ष पेश गर्ने,

(घ) संवेदनशील सूचना पूर्वाधारका धनीले अवलम्बन गरेको साइबर सुरक्षा अभ्यासको अनुगमन गर्ने,

(ङ) साइबर सुरक्षा सम्बन्धी प्राविधिक मापदण्ड तयार गरी निर्देशक समितिमा पेस गर्ने,

(च) साइबर सुरक्षा सम्बन्धी डिजिटल फोरेन्सिक ल्याव सञ्चालन गर्ने,

(छ) साइबर सुरक्षा सेवा प्रदायक अनुमतिपत्रको शर्त तथा मापदण्ड तर्जुमा गरी निर्देशक समिति समक्ष पेस गर्ने,

(ज) साइबर सुरक्षाका घटना सम्बन्धमा अन्य मुलुकका कम्प्यूटर आपतकालीन प्रतिकार्य समूहसँग समन्वय र सहकार्य गर्ने,

(झ) साइबर सुरक्षा सम्बन्धी प्रविधिको अनुसन्धान तथा विकासलाई प्रोत्साहन गर्ने तथा आवश्यकता अनुसार त्यस्ता कार्य गर्न विश्वविद्यालय तथा संघ संस्थाहरु सहितका राष्ट्रिय संस्थाहरुसंग सहकार्य गर्ने,

(ञ) साइबर सुरक्षा सम्बन्धमा आवश्यक समन्वय तथा सहकार्य गर्ने,

(ट) साइबर सुरक्षाको महत्व र आवश्यकताका सम्बन्धमा सचेतना अभिबृद्धि गर्ने,

(ठ) साइबर सुरक्षा सेवा प्रदायक अनुमतिपत्र प्रदान गर्ने,

(ड) कम्प्यूटर वा कम्प्यूटर प्रणालीको साइबर सुरक्षा निरीक्षण गर्ने,

(ढ) साइबर सुरक्षा सम्बन्धमा आवश्यक अन्य कार्य गर्ने गराउने।

96. **<u>निर्देशन दिन सक्नेः</u>** यो ऐन बमोजिमका कार्य कार्यान्वयन गर्न केन्द्रले आवश्यकता अनुसार संवेदनशील सूचना पूर्वाधारका धनी, अनुमतिपत्र प्राप्त सेवा प्रदायक तथा साइबर सुरक्षा परीक्षकलाई निर्देशन दिनेछ र त्यस्तो निर्देशनको पालना गर्नु सम्बन्धित संवेदनशील सूचना पूर्वाधारका धनी तथा अनुमतिपत्र प्राप्त सेवा प्रदायक व्यक्तिको कर्तव्य हुनेछ।

97. **<u>वार्षिक प्रतिवेदनः</u>** (१) केन्द्रले प्रत्येक आर्थिक वर्ष समाप्त भएको मितिले तीन महिना भित्र आफूले गरेको काम कारबाही सम्बन्धी प्रतिवेदन तयार गरी मन्त्रालय समक्ष पेश गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिमको प्रतिवेदनमा अन्य कुराका अतिरिक्त केन्द्रले प्राप्त गरेको बजेट तथा कार्यक्रम र कार्यक्रम सञ्चालन गर्दा हुन गएको लागत, कार्यक्रमबाट भएको उपलब्धि तथा भविष्यमा गर्नु पर्ने सुधार समेतका कुराहरु समावेश गर्नु पर्नेछ।

परिच्छेद- १०

<u>अनुमतिपत्र सम्बन्धी व्यवस्था</u>

98. **<u>साइबर सुरक्षा सेवा प्रदान गर्न अनुमतिपत्र लिनुपर्नेः</u>** (१) साइबर सुरक्षा सेवा प्रदान गर्न चाहने व्यक्ति, कम्पनी वा संस्थाले अनुमतिपत्र लिनु पर्नेछ।

(२) अनुमतिपत्रको किसिम, प्रत्येक अनुमतिपत्र प्राप्त गर्न आवश्यक योग्यता, अनुमतिपत्र दस्तुर, अनुमतिपत्र नवीकरण दस्तुर, अनुमतिपत्रका शर्त र सो सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

99. **<u>अनुमतिपत्रको लागि निवेदन दिनेः</u>** अनुमतिपत्र प्राप्त गर्न चाहने व्यक्ति, कम्पनी वा संस्थाले देहायको कागजात संलग्न गरी तोकिए बमोजिमको ढाँचामा केन्द्रमा निवेदन दिनु पर्नेछः-

(क) कम्पनी वा संस्थाको प्रबन्धपत्र र नियमावली,

(ख) कम्पनी वा संस्था दर्ताको प्रमाणपत्र,

(ग) कम्पनीको स्थायी लेखा नम्बर प्रमाणपत्र,

(घ) कम्पनी अद्यावधिक भएको पत्र,

(ङ) अघिल्लो आर्थिक वर्षको कर चुक्ता प्रमाणपत्र,

(च) कम्पनी वा संस्थाको सञ्चालक समितिको विवरण

(छ) सम्बन्धित व्यक्तिको नेपाली नागरिकताको प्रमाणपत्र वा राहदानी वा राष्ट्रिय परिचयपत्रको प्रतिलिपि,

(ज) तोकिए बमोजिमका अन्य कागजात।

100. **<u>जाँचबुझ गर्ने र अनुमतिपत्र दिनेः</u>** (१) दफा ११ बमोजिम प्राप्त निवेदन उपर जाँचबुझ गर्दा निवेदकले साइबर सुरक्षा प्रदान गर्ने सम्बन्धमा तोकिए बमोजिमको मापदण्ड पूरा गरेको देखिएमा त्यस्तो व्यक्ति वा संस्थालाई तीस दिनभित्र केन्द्रले अनुमतिपत्र प्रदान गर्नु पर्नेछ।

(२) अनुमतिपत्रको मान्य अवधि अनुमतिपत्र जारी भएको मितिले एक वर्षको हुनेछ।

(३) उपदफा (१) बमोजिम अनुमतिपत्र दिँदा त्यस्तो अनुमतिपत्र बमोजिम सञ्चालन गर्न पाउने साइबर सुरक्षा सेवा र सो सम्बन्धी शर्त तोकी अनुमतिपत्र दिइनेछ।

(४) अनुमतिपत्र प्राप्त व्यक्ति, कम्पनी वा संस्थाले साइबर सुरक्षा सम्बन्धी सेवा प्रदान गरेको विवरणको वार्षिक रुपमा तोकिए बमोजिमको ढाँचामा अभिलेख राख्नु पर्नेछ।

(५) अनुमतिपत्र दस्तुर, अनुमतिपत्र प्रदान गरिने ढाँचा र अनुमतिपत्र सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

101. **<u>अनुमतिपत्र नविकरणः</u>** (१) अनुमतिपत्र प्राप्त व्यक्तिले अनुमतिपत्रको अवधी समाप्त हुनुभन्दा कम्तीमा तीस दिन अघि अनुमतिपत्र नविकरण गर्नको लागि देहायका कागजात संलग्न गरी केन्द्रमा निवेदन दिनु पर्नेछः-

(क) सक्कल अनुमतिपत्र,

(ख) अनुमतिपत्र बमोजिम प्रदान गरेको साइबर सुरक्षा सेवाको वार्षिक विवरण,

(ग) कम्पनी वा संस्थाको हकमा कर चुक्ता प्रमाणपत्र, कम्पनी दर्ता प्रमाणपत्र,

(घ) व्यक्तिको हकमा नागरिकता प्रमाणपत्रको प्रतिलिपि र यस ऐन बमोजिमको कसूरमा सजाय नपाएको स्वघोषणा।

(२) उपदफा (१) बमोजिम प्राप्त निवेदन उपर जाँचबुझ गर्दा निवेदकले अनुमति प्रदान गर्दाका बखत तोकिएको शर्त पालना गरेको देखिएमा त्यस्तो अनुमतिपत्र एक वर्षको लागि नवीकरण गरि दिन सक्नेछ।

(३) अनुमतिपत्र नवीकरणको लागि दिइने निवेदन, नवीकरण दस्तुर, स्वघोषणा र सो सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

102. **<u>अभिलेख राख्नु पर्नेः</u>** (१) केन्द्रले अनुमतिपत्र प्राप्त गर्ने साइबर सुरक्षा सेवा प्रदायकको अनुमतिपत्रको किसिम छुट्टिने गरी साइबर सुरक्षा सेवा प्रदायकको अभिलेख राख्नु पर्नेछ।

(२) उपदफा (१) बमोजिमको अभिलेखलाई प्रत्यक आर्थिक वर्षको पहिलो महिनामा सार्वजनिक गर्नु पर्नेछ।

(३) अनुमतिपत्र प्राप्त व्यक्तिले साईवर सुरक्षा सम्बन्धी सेवा प्रदान गर्दा पटकै पिच्छे देहायका विवरण सहित अभिलेख राख्नु पर्नेछः

(क) अनुमतिपत्र प्राप्त व्यक्तिलाई साइबर सुरक्षा सेवामा लगाउने व्यक्ति वा संस्थाको नाम तथा ठेगाना,

(ख) अनुमतिपत्र प्राप्त व्यक्तिको तर्फबाट सेवा प्रदान गर्ने व्यक्तिको नाम,

(ग) साइबर सुरक्षा सेवा प्रदान गरिएको मिति,

(घ) प्रदान गरिएको सेवाको विवरण,

(ङ) तोकिए बमोजिमका अन्य विवरण।

(४) अनुमतिपत्र प्राप्त व्यक्तिले उपदफा (३) बमोजिमको विवरण सहितको वार्षिक अभिलेख केन्द्रलाई उपलव्ध गराउनु पर्नेछ र त्यस्तो अभिलेख तीन वर्ष सम्म सुरक्षित राख्नु पर्नेछ।

(५) वार्षिक अभिलेखको ढाँचा तोकिए बमोजिम हुनेछ।

103. **<u>अनुमतिपत्र खारेज वा निलम्बन गर्न सक्नेः</u>** (१) अनुमतिपत्र प्राप्त व्यक्तिले देहायको काम गरेमा केन्द्रले अनुमतिपत्र खारेज गर्ने, निलम्बन गर्ने वा चेतावनी दिन सक्नेछः-

(क) अनुमतिपत्र प्राप्त व्यक्तिले अनुमतिपत्रका शर्तहरु पालना नगरेमा,

(ख) झुट्टा विवरण दिई अनुमतिपत्र प्राप्त गरेमा,

(ग) अनुमतिपत्र प्राप्त व्यक्तिले टाट पल्टेको घोषणा गरेमा वा लिक्विडेसनमा गएमा,

(घ) अनुमतिपत्र प्राप्त व्यक्तिले यस ऐन अन्तर्गत वा किर्ते वा नैतिक पतन देखिने अपराधमा सजाय पाएमा।

(२) उपदफा (१) को खण्ड (क) वा (ख) बमोजिम कारबाही गर्नु अघि सम्बन्धित अनुमतिपत्र प्राप्त व्यक्तिलाई आफ्नो सफाई पेश गर्न पन्ध्र दिनको समय प्रदान गरिनेछ।

(३) उपदफा (२) बमोजिम दिइएको समयसीमाभित्र जवाफ प्राप्त नभएमा वा प्राप्त जवाफ चित्तबुझ्दो नभएमा केन्दले निजलाई चेतावनी दिन, निजको प्रमाणपत्र अवधि तोकी बढीमा एक वर्षको लागि निलम्बन गर्न वा प्रमाणपत्र खारेज गर्न सक्नेछ।

परिच्छेद— ११

<u>संवेदनशील सूचना पूर्वाधार सम्बन्धी व्यवस्था</u>

104. **<u>संवेदनशील सूचना पूर्वाधार तोक्नेः</u>** केन्द्रको सिफारिसमा नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशित गरी संवेदनशील सूचना पूर्वाधार तोक्न सक्नेछ।

105. **<u>संवेदनशील सूचना पूर्वाधार सम्बन्धी जानकारी माग गर्न सक्नेः</u>** (१) केन्द्रले संवेदनशील सूचना पूर्वाधारका धनीलाई लिखित सूचना दिई देहायका विषयमा जानकारी माग गर्न सक्नेछः-

(क) संवेदनशील सूचना पूर्वाधारको डिजाईन, कन्फिगुरेसन तथा सुरक्षा सम्बन्धी जानकारी,

(ख) संवेदनशील सूचना पूर्वाधारसँग जोडिएका वा संवेदनशील सूचना पूर्वाधारसँग सूचना आदान प्रदान गर्ने अन्य कम्प्यूटर वा कम्प्यूटर प्रणालीको डिजाईन, कन्फिगुरेसन तथा सुरक्षा सम्बन्धी जानकारी,

(ग) संवेदनशील सूचना पूर्वाधारसँग जोडिएका वा संवेदनशील सूचना पूर्वाधारसँग सूचना आदान प्रदान गर्ने अन्य कम्प्यूटर वा कम्प्यूटर प्रणालीको सञ्चालन सम्बन्धी जानकारी,

(घ) केन्द्रले संवेदनशील सूचना पूर्वाधारको साईवर सुरक्षा सुनिश्चित गर्ने क्रममा आवश्यक देखेका अन्य जानकारी।

(२) उपदफा (१) बमोजिम माग गरिएको जानकारी उपलव्ध गराउनु सूचना पूर्वाधारका धनीको कर्तव्य हुनेछ।

तर सूचना दिईएको संवेदनशील सूचना पूर्वाधारको धनीलाई प्रचलित नेपाल कानूनले कुनै प्रकारको जानकारी दिन छुट पाएको रहेछ भने निजले त्यस्तो जानकारी उपलव्ध गराउनु पर्ने छैन।

106. **<u>संवेदनशील सूचना पूर्वाधारको साइबर सुरक्षा अनुगमन र परीक्षण:</u>** (१) संवेदनशील सूचना पूर्वाधारको धनीले कम्तिमा वर्षको एक पटक संवेदनशील सूचना पूर्वाधारको सुरक्षा परीक्षण गराई र उक्त परीक्षणको प्रतिवेदन केन्द्र समक्ष पेश गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिम साइबर सुरक्षा परीक्षण गर्दा साइबर सुरक्षाका कुनै पक्षमा सन्तोषजनक किसिमले परीक्षण गरिएको छैन भन्ने कुरा केन्द्रलाई लागेमा केन्द्रले त्यस्ता छुट भएका पक्षका सम्बन्धमा परीक्षण गराउन निर्देशन दिन सक्नेछ। उक्त परीक्षणको प्रतिवेदन संवेदनशील सूचना पूर्वाधार धनीले केन्द्र समक्ष पेश गर्नु पर्नेछ।

(३) उपदफा (२) बमोजिमको सुरक्षा प्रतिवेदनमा केन्द्रलाई शंका लागेमा कारण सहितको लिखित जानकारी गराई केन्द्रले पुन: सुरक्षा परीक्षण गर्न गराउन सक्नेछ।

(४) केन्द्रले साइबर सुरक्षामा देखिएका कमी कमजोरी सुधार गर्न संवेदनशील सूचना पूर्वाधारका धनीलाई लेखी पठाउन सक्नेछ र त्यसरी लेखी आएमा संवेदनशील सूचना पूर्वाधारका धनीले आफ्नो कम्प्यूटर वा कम्प्यूटर प्रणालीमा देखिएका त्यस्ता कमी कमजोरी तत्कालै हटाउनु पर्नेछ।

(५) केन्द्रले संवेदनशील पूर्वाधारको अनुगमन गर्ने व्यवस्था गर्नेछ।

107. **<u>निर्देशन दिन सक्ने:</u>** (१) केन्द्रको सिफारिसमा निर्देशक समितिले समय समयमा संवेदनशील सूचना पूर्वाधारको साइबर सुरक्षा सम्बन्धमा संवेदनशील सूचना पूर्वाधारका धनीले पालना गर्नु पर्ने शर्त, सुरक्षाका उपायहरुका सम्बन्धमा निर्देशन दिन वा मापदण्ड बनाई लागू गर्न सक्नेछ।

(२) उपदफा (१) बमोजिम दिएको निर्देशन वा लागू गरेको मापदण्ड सार्वजनिक गर्नु पर्नेछ।

108. **<u>साइबर सुरक्षाका घटनाको जानकारी गराउनु पर्ने:</u>** संवेदनशील सूचना पूर्वाधारका धनीले साइबर सुरक्षाका घटना घटेमा त्यस्तो घटना घट्नासाथ देहायका विषयमा केन्द्रलाई जानकारी गराउनु पर्नेछ:–

(क) संवेदनशील सूचना पूर्वाधार प्रणालीको धनीले आफूले सञ्चालन गरेको संवेदनशील पूर्वाधार प्रणालीसंग सञ्चार आदान प्रदान गर्ने गरी जोडिएको कुनै कम्प्यूटर वा कम्प्यूटर प्रणालीसँग सम्बन्धीत तोकिएको साइबर सुरक्षा घटना,

(ख) संवेदनशील सूचना पूर्वाधारसंग सम्बन्धित साइबर सुरक्षा सम्बन्धी अन्य कुनै किसिमको घटना।

109. **<u>साइबर सुरक्षा अभ्यास गराउनुपर्ने:</u>** (१) संवेदनशील सूचना पूर्वाधारका धनीले कुनै महत्वपूर्ण साइबर सुरक्षा घटना प्रतिक्रिया गर्न तत्पर अवस्थामा राखे नराखेको परीक्षण गर्न समय समयमा साइबर सुरक्षा अभ्यास गर्नुपर्नेछ।

(२) संवेदनशील सूचना पूर्वाधारका धनीले केन्द्रले सञ्चालन गर्ने साइबर सुरक्षा अभ्यासमा सहभागी हुनुपर्नेछ।

परिच्छेद-१२
<u>साइबर सुरक्षा परीक्षण र परीक्षक सम्बन्धी व्यवस्था</u>

110. **<u>साइबर सुरक्षा परीक्षक दर्ता हुनुपर्ने:</u>** (१) साइबर सुरक्षा परीक्षण गर्ने व्यक्ति वा संस्थाले साइबर सुरक्षा परीक्षकको रुपमा काम गर्नको लागि केन्द्रमा सूचीकृत हुनु पर्नेछ।

(२) यो ऐन प्रारम्भ हुनुअघि प्रचलित कानून बमोजिम दर्ता भई साइबर सुरक्षा परीक्षण गरिरहेका व्यक्ति वा संस्था यो ऐन प्रारम्भ भएको नब्बे दिनभित्र केन्द्रमा सूचीकृत हुनु पर्नेछ।

(३) केन्द्रले कम्तीमा वार्षिक एक पटक यो सूची अध्यावधिक गर्नेछ।

(४) साइबर सुरक्षा परीक्षकका रुपमा सूचीकृत हुन केन्द्र समक्ष निम्न कागजातहरू पेश गर्नुपर्नेछः-

(क) संस्था दर्ताको प्रमाणपत्र

(ख) VAT /PAN दर्ताको प्रमाणपत्र

(ग) करचुक्ताको प्रमाणपत्र

(५) सूचीकरणका लागि आवश्यक योग्यता तथा मापदण्डहरु तोकिए बमोजिमको हुनेछ।

111. **<u>साइबर सुरक्षा परीक्षकका कार्यहरू:</u>** साइबर सुरक्षा परीक्षकले गर्ने कार्यहरू देहाय बमोजिम हुनेछः-

(क) सेक्युरिटी पोष्चर एसिस्मेन्ट

(ख) भल्नेरेबिलीटी एसिस्मेन्ट

(ग) पेनिट्रेसन टेस्टिङ्ग

(घ) डाटाबेस सेक्युरिटी एसिस्मेन्ट

(ङ) नेटवर्क सेक्युरिटी टेस्टिङ्ग

(च) साइबर सेक्युरिटी अडिट

(छ) रिस्क एसिस्मेन्ट

(ज) तोकिएका अन्य कार्य।

112. **<u>सूचीकृत गर्नुपर्ने:</u>** साइबर सुरक्षासँग सम्बन्धित भनी केन्द्रले तोकेको हार्डवयर उत्पादन र आपूर्ति सम्बन्धी कार्य गर्ने व्यक्ति, साइबर सुरक्षासँग सम्बन्धित भनी केन्द्रले तोकेको सफ्टवेयर विकास र आपूर्ति सम्बन्धी कार्य गर्ने व्यक्ति र सो हार्डवयर तथा सफ्टवेयर सञ्चालनका सम्बन्धमा परामर्श तथा अन्य सेवा उपलब्ध गर्ने व्यक्ति केन्द्रमा सूचीकृत हुनु पर्नेछ।

परिच्छेद- १३

<u>सूचना प्रविधि तालिम केन्द्र सम्बन्धी व्यवस्था</u>

113. **<u>सूचना प्रविधि तालिम केन्द्र</u>** : (१) सूचना प्रविधि क्षेत्रका साईबर सुरक्षा, सुरक्षा परीक्षण, डाटावेस, हार्डवेयर, नेटवर्क, प्रोग्रामिङ्ग, सफ्टवेयर, वेभ एप्लिकेशन, मोबाईल एप्लिकेशन, सर्भर व्यवस्थापन, क्लाउड सेवा सञ्चालन, साईबर फरेन्सिक, डाटा सेन्टर, आर्टिफिसियल ईन्टेलिजेन्स, मेसिन लर्निङ्ग, क्वालिटी एसुरेन्स, सूचना प्रविधि व्यवस्थापन लगायतका नवीनतम प्रविधि सम्बन्धी तालिम, अध्ययन तथा अनुसन्धान र यस क्षेत्रसँग सम्बन्धित जनशक्तिको दक्षता अभिवृद्धि गर्न मन्त्रालय अन्तर्गत राष्ट्रिय स्तरको सूचना प्रविधि तालिम केन्द्र रहनेछ।

(२) केन्द्रको प्रमुखको रुपमा कार्य गर्नको लागि मन्त्रालयले तोकेको सेवा / समूहको राजपत्राङ्कित प्रथम श्रेणीको अधिकृत रहनेछन्।

(३) केन्द्र सञ्चालनको लागि आवश्यक प्राविधिक तथा प्रशासनिक कर्मचारी नेपाल सरकारले व्यवस्था गर्नेछ।

114. **<u>केन्द्रको काम, कर्तव्य र अधिकार:</u>** सूचना प्रविधि तालिम केन्द्रको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) सूचना प्रविधि सम्बन्धी ज्ञान विस्तार गर्न राष्ट्रियस्तरमा सूचना प्रविधि सम्बन्धी तालिम प्रदान गर्ने,

(ख) सूचना प्रविधि सम्बन्धी सेवाकालीन तालिम सञ्चालन गर्ने,

(ग) सूचना प्रविधि सम्बन्धी नवीनतम क्षेत्रमा अध्ययन तथा अनुसन्धान गर्ने,

(घ) सूचना प्रविधि सम्बन्धी सबै किसिमको तालिम कार्यक्रम सञ्चालन गर्ने गराउने,

(ङ) नेपाल सरकारले तोकेका सूचना प्रविधि सम्बन्धी अन्य कार्यहरु गर्ने।

परिच्छेद-१४

<u>साइबर स्पेशमा निषेधित कार्यहरू</u>

115. **<u>साइबर बुलिङ्ग गर्न नहुने:</u>** कसैले विद्युतीय प्रणालीको प्रयोग गरी अर्को व्यक्तिलाई हैरानी गर्ने, जिस्क्याउने, होच्याउने, हतोत्साहित गर्ने, अपमान गर्ने वा हप्काउने जस्ता कार्य गर्न गराउन हुँदैन।

116. **<u>यौनजन्य दुर्व्यवहार गर्न नहुने:</u>** कसैले पनि विद्युतीय प्रणाली मार्फत कसैलाई प्रचलित कानून बमोजिम यौनजन्य दुर्व्यवहार मानिने कुनै कार्य गर्न वा सोको लागि कसैलाई अनुचित प्रलोभनमा पार्ने वा धम्की दिने जस्ता कुनै कार्य गर्न वा गराउन हुँदैन।

117. **<u>अश्लील सामाग्री उत्पादन, संकलन, वितरण, प्रकाशन, प्रदर्शन, प्रसार वा खरिद विक्रि गर्न वा गराउन नहुनेः</u>** कसैले विद्युतीय प्रणालीको माध्यमबाट कुनै अश्लिल सामग्रीको उत्पादन, संकलन गर्न, उपलव्ध रहेको जानकारी संप्रेषण गर्न, देखाउन, वितरण गर्न, प्रकाशन गर्न, प्रदर्शन गर्न, प्रसार गर्न वा विक्री गर्न वा संचय गर्न हुँदैन।

तर कुनै व्यक्तिले कुनै अनुसन्धान, कानून कार्यान्वयन, अध्यापन वा चिकित्साकीय प्रयोजनको लागि बाल यौनजन्य सामग्रीको संप्रेषण, प्राप्ति, वा संचय गरेको यथोचित रुपमा पुष्टि गरेमा र त्यस्तो उद्देश्य पूरा हुनासाथ त्यस्ता सामग्री मेटाएमा यस दफा बमोजिमको कसूर मानिने छैन।

118. **<u>प्रलोभनमा पार्न नहुनेः</u>** कसैले विद्युतीय प्रणालीको माध्यमबाट वा सो प्रणालीको उपयोग गरेर कसैलाई यौन शोषण गर्ने वा ठगी गर्ने वा अरु कुनै गैर कानूनी कार्य गर्ने मनसाय राखी कुनै प्रस्ताव राख्न, प्रलोभन पार्न, भेट्न, वा कुनै गैरकानूनी गतिविधिमा लाग्न, उक्साउन वा सोको लागि अनलाईन सम्बन्ध स्थापित गर्न प्रस्ताव गर्न हुँदैन।

119. **<u>गोप्य कोड चोरी गर्न नहुनेः</u>** कसैले विद्युतीय माध्यमबाट फिसिङ तथा स्पुफिङ लगायतका विधि प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीको पासवर्ड, पिनकोड, प्याटर्न तथा टोकन लगायतका गोप्य कोड चोरी गर्नु वा गराउनु हुँदैन।

<u>स्पष्टीकरणः</u> कसैले सामाजिक सञ्जाल, इमेल वा वेबसाइट मार्फत नक्कली लिङ्क प्रयोग गरी साइबर स्पेसका प्रयोगकर्तालाइ झुक्याई संवेदनशील जानकारी प्रवाह गर्न प्रेरित गर्ने वा कुनै मालवेयर स्थापना गर्ने कार्य गरेमा फिसिङ्ग गरेको मानिनेछ।

कसैले अज्ञात स्रोतबाट भएको सञ्चारलाई ज्ञात र विश्वसनीय स्रोतबाट आएको भनी झुक्याउने कार्य गरेमा स्पूफिङ गरेको मानिनेछ।

120. **<u>कम्प्युटर प्रणालीमा अनधिकृत पहुँच पुर्याउन नहुनेः</u>** कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीमा अनाधिकृत पहुँच पुर्याउने कार्य गर्नु वा गराउनु हुँदैन।

121. **<u>कम्प्युटर प्रणालीबाट डाटा चोरी गर्न नहुनेः</u>** कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीबाट डाटा चोरी गर्ने कार्य गर्नु वा गराउनु हुँदैन। यसका साथै नेटवर्कमा प्रसारित डाटालाई स्निफिङ लगायतका विधिहरु प्रयोग गरी डाटा चोरी गर्न वा गराउनु हुँदैन।

<u>स्पष्टीकरणः</u> कसैले दुई वा सोभन्दा बढी पक्षहरुबीच भएको डाटा आदान प्रदानमा सम्बधित पक्षको अनुमतिबिना अनाधिकृत रुपमा उक्त डाटा सुन्ने, पढ्ने वा हेर्ने कार्य गरेमा स्निफिङ गरेको मानिनेछ।

122. **<u>कम्प्युटर प्रणालीमा रहेका डाटा हेरफेर गर्न वा मेटाउन नहुनेः</u>** कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीमा प्रवेश गरी डाटाको अखण्डतामा फरक पर्ने गरी डाटा हेरफेर गर्ने वा मेटाउने कार्य गर्नु वा गराउनु हुँदैन।

123. **<u>कम्प्युटर प्रणालीमा अवान्छित एपलिकेशन/प्रोग्राम फैलाउन नहुनेः</u>** कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको कम्प्युटर वा कम्प्युटर प्रणालीमा अनुमतिबिना अवान्छित एपलिकेशन/प्रोग्राम प्रवेश गराउने/फैलाउने कार्य गर्नु वा गराउनु हुँदैन।

124. **<u>सार्वजनिक सूचना प्रणाली सार्वजनिक प्रयोगका लागि उपलब्ध हुन अवरोध गर्न नहुने:</u>** कसैले अर्काको कम्प्यूटर वा कम्प्यूटर प्रणालीको सञ्चाललाई डिनायल अफ सर्भिस लगायतका विधि प्रयोग गरी बन्द गर्ने वा कम्प्यूटर प्रणालीको अपेक्षित प्रयोगकर्ताहरूका लागि कम्प्यूटर प्रणालीमा पहुँच नपुग्ने वातावरण सिर्जना हुने कार्य गर्नु वा गराउनु हुँदैन।

<u>स्पष्टीकरण:</u> कसैले सार्वजनिक रुपमा सेवा प्रदान गर्ने कम्प्युटर प्रणाली बन्द गर्ने वा उक्त प्रणालीबाट प्रदान गरिने सेवा अवरुद्ध हुने गरी आक्रमण गर्ने कार्य गरेमा डिनायल-अफ-सर्भिस आक्रमण गरेको मानिनेछ।

125. **<u>इन्टरनेट अफ थिंग्समा आक्रमण गर्न नहुने:</u>** कसैले इन्टरनेट अफ थिंग्समा बिना अनुमति सो सँजालको निर्धारित काममा खलल पुर्याउने कार्य गर्नु वा गराउनु हुँदैन।

<u>स्पष्टीकरण</u>: एक अर्का बीच डाटा आदानप्रदान गर्न सक्ने इलेक्ट्रोमेकानिकल उपकरणहरूको सामूहिक सञ्चाललाई इन्टरनेट अफ थिंग्स भन्ने बुझिन्छ।

126. **<u>विद्युतीय प्रणालीको दुरुपयोग गर्न नहुने:</u>** (१) कसैले विद्युतीय माध्यमको प्रयोग गरी नागरिकहरुका बीच वर्गीय, जातीय, धार्मिक, क्षेत्रीय, साम्प्रदायक र यस्तै अरु कुनै आधारमा घृणा, द्वेष वा अवहेलना उत्पन्न हुने कुनै काम कारबाही गर्न वा बिभिन्न जात, जाती वा सम्प्रदाय बीचको सम्बन्ध खलल गर्नु वा गराउनु हुँदैन।

(२) कसैले विद्युतीय माध्यमको प्रयोग जातीय भेदभाव वा छुवाछुतलाई दुरुत्साहन दिने, श्रमप्रति अवहेलना गर्ने, अपराध गर्न दुरुत्साहन गर्ने ,शान्ति सुरक्षा भङ्ग हुने कार्यलाई बढावा दिने वा प्रचलित कानून बमोजिम प्रकाशन वा प्रसारण गर्न रोक लगाएको कुरा प्रशारण वा संप्रेषण गर्ने वा सार्वजनिक सदाचार र नैतिकताको प्रतिकूल हुने कुनै कार्य गर्न वा गराउन हुँदैन।

(३) कसैले मानव बेचविखन तथा अपहरण वा लागू औषध बिक्री वितरण वा प्रचलित कानूनले अपराधको रुपमा निषेध गरेको कार्य गर्न वा गराउन विद्युतीय प्रणालीको प्रयोग गर्न हुँदैन।

(४) कसैले प्रचलित कानुनले बिक्री तथा वितरण गर्न निषेध गरेको सामाग्री बिक्री गर्न वा सो सम्बन्धमा विज्ञापन प्रकाशन, प्रशारण वा प्रदर्शन गर्न विद्युतीय प्रणालीको प्रयोग गर्न हुँदैन।

127. **<u>मुलुकको सुरक्षा वा तथ्यांक प्रणालीमा अवरोध सृजना गर्न नहुने:</u>** कसैले विद्युतीय प्रणालीको प्रयोग गरी नेपालको राष्ट्रिय सुरक्षा, सार्वभौमसत्ता, भौगोलिक अखण्डता, राष्ट्रियता वा राष्ट्रिय एकता, स्वाधीनता, स्वाभिमान वा सङ्घीय इकाई बीचको सुसम्बन्ध खलल पार्ने वा मुलुकको सुरक्षा वा तथ्यांक प्रणालीमा अवरोध सृजना गर्ने वा प्रतिकूल असर पार्ने कुनै कार्य गर्न वा गराउन हुँदैन।

128. **<u>आर्टिफिसियल इन्टेलिजेन्सको दुरुपयोग गर्न नहुने:</u>** यस ऐन बमोजिम कसूर मानिने कार्यहरु आर्टिफिसियल इन्टेलिजेन्सको प्रयोग गरी समेत गर्न हुँदैन।

परिच्छेद-१५

<u>कसूर तथा सजाय</u>

129. **<u>कसूर गरेको मानिने</u>**: कसैले देहायको कुनै कार्य गरे गराएमा यस ऐन अन्तर्गतको कसूर गरेको मानिनेछ;-

(क) दफा १७ विपरीत सूचना प्रविष्टि, सम्प्रेषण वा हेरफेर गरेमा, मेटाएमा, विद्युतीय प्रणालीको कार्य सञ्चालनमा हस्तक्षेप गरेमा वा वित्तीय सूचना प्राप्त गरेमा,

(ख) दफा १९ विपरीत कुनै प्रोग्राम संप्रेषण वा सञ्चालन गरेमा,
(ग) दफा ४० विपरीत झुट्टा व्यहोराको सूचना पेस गरेमा,
(घ) दफा ४२ बमोजिम तोकिएको म्यादभित्र विवरण, कागजात वा प्रतिवेदन दाखिला नगरेमा वा सुरक्षित राख्नु पर्ने किताब, रजिष्टर, स्रेस्ता, लेखा आदि सुरक्षित तथा रीतपूर्वक नराखेमा,
(ङ) दफा ४८ विपरीत झुट्टा प्रमाणपत्र पेश गरेमा,
(च) दफा ५३ विपरीत पहिचानको दुरुपयोग गरेमा,
(छ) दफा ५४ विपरित विद्युतीय प्रणालीमा अवरोध गरेमा,
(ज) दफा ६४ को उपदफा (४) विपरीत भेटिङ्ग नगराई सफ्टवेयर र हार्डवेयर प्रणाली खरिद र प्रयोग गरेमा,
(झ) दफा ६७ को उपदफा (३) विपरीत सुरक्षित नामहरुसँग बाझिने किसिमले मिल्दोजुल्दो वा महत्वलाई अवमुल्यन गर्ने डोमेन नाम दर्ता गरेमा,
(ञ) दफा ७१ विपरीत अनाधिकृत रुपले डोमेन नाम प्रणाली सञ्चालन गरेमा,
(ट) दफा ७४ विपरीत अनुमति नलिई वा अनुमति लिएको अवधि भन्दा वढी अवधि उपकरणहरु प्रयोग गरेमा,
(ठ) दफा ८० विपरीत वैयक्तिक विवरण सङ्कल गरेमा,
(ड) दफा ८६ विपरीत इजाजत नलिई डाटा सेन्टर वा क्लाउड सञ्चालन गरेमा,
(ढ) दफा ८८ विपरीत विद्युतीय स्वरुपको सूचनालाई क्षति पुऱ्याएमा वा अवरोध गरेमा,
(ण) दफा ८९ विपरीत गोपनीयता भङ्ग गरेमा,
(थ) दफा ९० विपरीत विद्युतीय प्रणालीको श्रोत सङ्केत नष्ट, परिवर्तन वा चोरी गरेमा,
(द) दफा ९१ विपरीत विद्युतीय प्रणालीमा रहेको सूचना चोरी गरेमा,
(ध) दफा ९३ बमोजिमको अवधिसम्म विवरणहरु सुरक्षित नराखेमा,
(न) दफा ९६ बमोजिम केन्द्रले दिएको निर्देशन पालना नगरेमा,
(प) दफा ९८ बमोजिम अनुमतिपत्र नलिई वा दफा १०३ बमोजिम खारेज वा निलम्बन भएको अनुमतिपत्र प्रयोग गरी साइबर सुरक्षा सेवा प्रदान गरेमा,
(फ) दफा १०८ बमोजिम साइबर सुरक्षाको घटनाको जानकारी नगराएमा,
(ब) दफा ११५ विपरीत साइबर बुलिङ्ग गरेमा,
(भ) दफा ११६ विपरीत यौनजन्य दुर्व्यवहार गरेमा,
(म) दफा ११७ विपरीत अश्लील सामाग्री उत्पादन, संकलन, वितरण, प्रकाशन, प्रदर्शन, प्रसार वा खरिद विक्रि गर्ने वा गराउने कार्य गरेमा,
(य) दफा ११८ विपरीत प्रलोभनमा पार्ने कार्य कार्य गरेमा,
(र) दफा ११९ विपरीत गोप्य कोड चोरी गरेमा,
(ल) दफा १२० विपरीत कम्प्युटर प्रणालीमा अनधिकृत पहुँच पुर्याउने कार्य गरेमा,
(व) दफा १२१ विपरीत कम्प्युटर प्रणालीबाट डाटा चोरी गर्ने कार्य गरेमा,
(श) दफा १२२ विपरीत कम्प्युटर प्रणालीमा रहेका डाटा हेरफेर गर्न वा मेटाउने कार्य गरेमा,
(ष) दफा १२३ विपरीत कम्प्युटर प्रणालीमा अवान्छित एपलिकेशन/प्रोग्राम फैलाउने कार्य गरेमा,

(स) दफा १२४ विपरीत सार्वजनिक रुपमा सञ्चालनमा ल्याइएको प्रणाली सार्वजनिक प्रयोगका लागि उपलब्ध हुन अवरोध गरेमा,

(ह) दफा १२५ विपरीत इन्टरनेट अफ थिंग्समा आक्रमण गरेमा,

(क्ष) दफा १२६ विपरीत विद्युतीय प्रणालीको दुरुपयोग गरेमा,

(त्र) दफा १२७ विपरीत मुलुकको सुरक्षा वा तथ्यांक प्रणालीमा अवरोध सृजना गरेमा,

(ज्ञ) दफा १२८ विपरीत आर्टिफिसियल इन्टेलिजेन्सको दुरुपयोग गरेमा।

130. **<u>सजाय</u>**ः कसैले दफा १२९ बमोजिमको कसूर गर्ने वा गराउनेलाई देहाय बमोजिमको सजाय हुनेछः-

(क) दफा १२९ को खण्ड (क) बमोजिमको कसूरमा पाँच लाख रुपैँया सम्म जरिवाना वा तीन वर्षसम्म कैद वा दुवै सजाय,

(ख) दफा १२९ को खण्ड (ख), बमोजिमको कसूरमा तीन लाख रुपैँया सम्म जरिवाना वा तीन वर्षसम्म कैद वा दुवै सजाय,

(ग) दफा १२९ को खण्ड (ग) बमोजिमको कसूरमा तीन लाख रुपैँया सम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय,

(घ) दफा १२९ को खण्ड (घ) बमोजिमको कसूरमा एक लाख रुपैँया सम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय,

(ङ) दफा १२९ को खण्ड (ङ) बमोजिमको कसूरमा तीन लाख रुपैँया सम्म जरिवाना वा तीन वर्षसम्म कैद वा दुवै सजाय,

(च) दफा १२९ को खण्ड (च) बमोजिमको कसूरमा तीन लाख रुपैँया सम्म जरिवाना वा तीन वर्षसम्म कैद वा दुवै सजाय,

(छ) दफा १२९ को खण्ड (छ) बमोजिमको कसूरमा पाँच लाख रुपैँया सम्म जरिवाना वा तीन वर्षसम्म कैद वा दुवै सजाय,

(ज) दफा १२९ को खण्ड (ज) बमोजिमको कसूरमा पाँच लाख रुपैँया सम्म जरिवाना,

(झ) दफा १२९ को खण्ड (झ) बमोजिमको कसूरमा पाँच लाख रुपैँया सम्म जरिवाना,

(ञ) दफा १२९ को खण्ड (ञ) बमोजिमको कसूरमा एक लाख रुपैँया सम्म जरिवाना वा छ महिनासम्म कैद वा दुवै सजाय,

(ट) दफा १२९ को खण्ड (ट) बमोजिमको कसूरमा एक लाख रुपैँया सम्म जरिवाना,

(ठ) दफा १२९ को खण्ड (ठ) बमोजिमको कसूरमा तीन लाख रुपैँया सम्म जरिवाना वा तीन वर्षसम्म कैद वा दुवै सजाय,

(ड) दफा १२९ को खण्ड (ड) बमोजिमको कसूरमा पाँच लाख रुपैँया सम्म जरिवाना,

(ढ) दफा १३० को खण्ड (ढ) बमोजिमको कसूरमा दश लाख रुपैँया सम्म जरिवाना वा पाँच वर्षसम्म कैद वा दुवै सजाय,

(ण)दफा १२९ को खण्ड (ण) बमोजिमको कसूरमा तीन लाख रुपैँया सम्म जरिवाना वा तीन वर्षसम्म कैद वा दुवै सजाय,

(त) दफा १२९ को खण्ड (त) बमोजिमको कसूरमा दश लाख रुपैँया सम्म जरिवाना वा पाँच वर्षसम्म कैद वा दुवै सजाय,

(थ)दफा १२९ को खण्ड (थ) बमोजिमको कसूरमा दश लाख रुपैँया सम्म जरिवाना वा पाँच वर्षसम्म कैद वा दुवै सजाय,

(द)दफा १२९ को खण्ड (द) बमोजिमको कसूरमा कसूरको मात्रा हेरी दश लाख रुपैँया सम्म जरिवाना,

(ध)दफा १२९ को खण्ड (ध) बमोजिमको कसूरमा पन्ध्र हजार रुपैँया सम्म जरिवाना,

(न)दफा १२९ को खण्ड (न) बमोजिमको कसूरमा एक लाख रुपैँया सम्म जरिवाना वा तीन महिनासम्म कैद वा दुवै सजाय,

(प) दफा १२९ को खण्ड (प) बमोजिमको कसूरमा पन्ध्र हजार रुपैँया सम्म जरिवाना,

(फ) खण्ड (क), (ख), (ग), (घ), (ङ), (च), (छ) (ज), (झ), (य), (ट), (ठ), (ड), (ढ), (ण), (त), (थ), (द), (ध), (न) र (प) मा लेखिएदेखि बाहेक दफा १२९ बमोजिमको अन्य कसूरमा कसूरको मात्रा हेरी दुईलाख रुपैयाँसम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय।

131. **<u>जफत हुनेः</u>** दफा १२९ को खण्ड (ट) र (न) बमोजिमको कसूर गर्न प्रयोग भएको सामग्री जफत हुनेछ।

132. **<u>कसूर गर्न दुरुत्साहन गर्न नहुनेः</u>** कसैले यस ऐन बमोजिमको कुनै कसूर गर्न कसैलाई दुरुत्साहन गरेमा वा त्यस्तो कसूर गर्न उद्योग गरेमा वा षडयन्त्रमा संलग्न भएमा त्यस्तो व्यक्तिलाई मुख्य कसूरदारलाई भए सरहको सजाय हुनेछ।

133. **<u>मतियारलाई हुने सजायः</u>** यस ऐन बमोजिमको कुनै कसूर गर्न सघाउने वा अन्य कुनै व्यहोराले मतियार भई कार्य गर्ने व्यक्तिलाई मुख्य कसूरदारलाई भएको सजायको आधा सजाय हुनेछ।

134. **<u>सङ्गठित संस्थाबाट भएको कसूरः</u>** कुनै फर्म वा कम्पनी वा सङ्गठित संस्थाले यस ऐन वा कानून बमोजिम कसूर मानिने कुनै काम गरे वा गराएमा त्यस्तो कार्य गर्ने गराउने व्यक्ति जिम्मेवार हुनेछ र त्यस्तो व्यक्ति किटान हुन नसकेमा फर्मको हकमा सम्बन्धित धनी वा हिस्सेदारहरु, कम्पनी वा सङ्गठित संस्थाको हकमा सम्बन्धित धनी, हिस्सेदारहरु, संचालक, प्रबन्ध संचालक वा महाप्रबन्धक र त्यस्तो व्यक्ति पनि किटान हुन नसकेमा त्यस्तो संस्थाको कार्यकारी प्रमुखले आपराधिक दायित्व व्यहोर्नु पर्नेछ।

135. **<u>प्रचलित कानून बमोजिम सजाय गर्न बाधा नपर्नेः</u>** यस ऐन अन्तर्गत कसूर ठहरिने कुनै काम अन्य कुनै प्रचलित कानून बमोजिम पनि कसूर ठहरिने रहेछ भने त्यस्तो कसूर उपर छुट्टै कारबाही चलाई सजाय गर्न यस ऐनले बाधा पुऱ्याएको मानिने छैन।

136. **क्षतिपूर्ति भराउनु पर्नेः** यस ऐन बमोजिम कसूर गरेको कारणबाट कसैलाई कुनै किसिमको हानी, नोक्सानी, हैरानी वा क्षती भएको रहेछ भने त्यस्तो हानी, नोक्सानी हैरानी वा क्षतिको क्षतिपूर्ति सम्बन्धित कसूरदारबाट भराई दिनु पर्नेछ।

137. **नेपाल सरकार वादी हुनेः** (१) यस ऐन बमोजिमको कसूरसँग सम्बन्धित मुद्दामा नेपाल सरकार वादी हुनेछ।

(२) उपदफा (१) बमोजिमको मुद्दा मुलुकी फौजदारी कार्यविधि संहिता, २०७४ को अनुसूची-१ मा समावेश भएको मानिनेछ।

138. **उजुर गर्ने हदम्यादः** यो ऐन बमोजिम कसूर ठहर्ने कुनै कुरा भएकोमा त्यस्तो उल्लंघन वा कसूर भए गरेको थाहा पाएको मितिले नब्बे दिन भित्र उजुर गर्नु पर्नेछ।

139. **मुद्दा हेर्ने अधिकारीः** यस ऐन बमोजिमको कसूरसँग सम्बन्धित मुद्दाको कारवाही र किनारा गर्ने अधिकार न्यायाधिकरणलाई हुनेछ।

140. **पुनरावेदन लाग्न सक्नेः** (१) न्यायाधिकरणले गरेको निर्णय वा अन्तिम आदेश उपर चित्त नबुझ्ने पक्षले त्यस्तो आदेश वा निर्णय भएको मितिले नब्बे दिनभित्र सम्बन्धित उच्च अदालत समक्ष पुनरावेदन दिन सक्नेछ।

(२) उपदफा (१) बमोजिमको उच्च अदालतले पुनरावेदन सुन्नको लागि साइबर सुरक्षा सम्बन्धी विशेष ईजलास तोक्नु पर्नेछ।

परिच्छेद-१६

अनुसन्धान तथा प्रमाण

141. **अनुसन्धान अधिकृतः** यस ऐन बमोजिमको कसूर सम्बन्धी मुद्दाको अनुसन्धान सूचना प्रविधि सम्बन्धी ज्ञान भएको कम्तीमा प्रहरी निरिक्षक स्तरको अधिकारीले गर्नेछ।

142. **विद्युतीय प्रमाणको ग्राह्यताः** प्रचलित कानून बमोजिम कुनै पनि कसूर विरुद्धको कारबाहीको क्रममा विद्युतीय प्रणालीबाट सिर्जना भएको विद्युतीय वा अन्य कुनै स्वरुपमा रहेको कुनै सूचना वा तथ्याङ्क प्रमाणको रुपमा ग्राह्य हुनेछ।

143. **खानतलासी तथा जफतः** (१) अनुसन्धान अधिकृतले कुनै कसूर प्रमाणित गर्न प्रमाणमा लाग्न सक्ने कुनै विद्युतीय उपकरण वा सूचना वा अन्य त्यस्तै वस्तु रहेको स्थानमा प्रवेश गरी खानतलासी लिन, विद्युतीय उपकरण वा सूचना वा अन्य त्यस्तै वस्तु जफत गर्नु परेमा अदालतको अनुमति लिनु पर्नेछ।

(२) उपदफा (१) बमोजिमको खानतलासी तथा जफतका लागि अनुमति लिन अनुसन्धान अधिकृतले त्यस्तो खानतलासी तथा जफत गर्न आवश्यक रहेको पुष्टि गर्ने तत्काल प्राप्त प्रमाण वा विश्वसनीय आधार सहित अदालत समक्ष निवेदन दिनु पर्नेछ।

(३) उपदफा (२) बमोजिमको निवेदनसाथ प्राप्त प्रमाण तथा आधारमा अदालत विश्वस्त भएमा उपदफा (१) बमोजिमको खानतलासी तथा जफतको लागि अनुसन्धान अधिकृतलाई अनुमति दिन सक्नेछ।

(४) अनुसन्धान अधिकृतले उपदफा (१) बमोजिम खानतलासी वा जफत गर्दा देहाय बमोजिमको कार्य यथाशिघ्र गर्नु पर्नेछः-

(क) जफत गरेको मिति र समय खुलाई कब्जामा लिएको वस्तुहरुको सूचि तयार गर्ने,

(ख) खण्ड (क) बमोजिमको सूचिको एक प्रति नक्कल उक्त वस्तुहरुको स्वामित्व रहेको व्यक्तिलाई दिने,

(ग) खानतलासी गरिएको स्थान नियन्त्रणमा राख्ने,

(घ) कब्जामा लिएको वस्तुहरुको संरक्षणको प्रत्याभूति गर्ने।

(५) अदालतबाट आदेश भई आएमा विद्युतीय उपकरण नियन्त्रण वा जिम्मामा रहेको व्यक्ति वा निजको अख्तियारवाला कुनै व्यक्तिलाई उक्त विद्युतीय उपकरणमा रहेको कुनै विद्युतीय प्रणालीमा रहेको सूचनामा पहुँच प्राप्त गर्न वा उक्त सूचनाको प्रतिलिपी दिनुपर्नेछ।

(६) उपदफा (१) बमोजिम खानतलासी लिने अनुसन्धान अधिकृतलाई खानतलास गरिएको सूचना अर्को कुनै विद्युतीय प्रणालीमा रहेको वा त्यस्तो प्रणालीको कुनै अंश क्षेत्राधिकार भित्रै रहेको अर्को कुनै प्रणालीमा रहेको वा त्यस्तो सूचना प्रारम्भिक प्रणालीबाट कानून बमोजिम पहुँच राख्न सकिने अर्को प्रणालीमा रहेको विश्वास लागेमा निजले यथाशिघ्र त्यस्तो खानतलासी विस्तार गरी त्यस्तो प्रणालीमा पहुँच राख्न सक्नेछ।

144. **<u>सहयोग गर्नु पर्नेः</u>** अनुसन्धान अधिकृतले खानतलासीको क्रममा कुनै विद्युतीय उपकरण वा सूचना उक्त मुद्दामा आरोपित नरहेको व्यक्तिको कब्जा वा नियन्त्रणमा रहेको पाएमा त्यस्तो व्यक्तिले अनुसन्धान अधिकृतलाई विद्युतीय उपकरण वा विद्युतीय तथ्याङ्कसम्मको पहुँच पु-याउन वा प्रयोग गर्न वा प्रतिलिपि उतार गर्न, ईन्क्रिप्ट गरिएको सूचनालाई डिक्रिप्ट गर्न अनुमति दिई अन्य आवश्यक सहयोग गर्नु पर्नेछ।

145. **<u>झिकाउने आदेशः</u>** (१) कुनै कसूरको अनुसन्धान वा अभियोजन प्रयोजनको लागि कुनै खास विद्युतीय प्रणाली, सूचना वा उपकरण आवश्यक रहेको कुरामा अदालत समक्ष पेश भएको प्रमाणको आधारमा अदालत विश्वस्त भएमा त्यस्तो विद्युतीय प्रणाली, सूचना वा उपकरण नियन्त्रणमा राखेको व्यक्तिलाई उक्त विद्युतीय प्रणाली, सूचना वा उपकरण पेश गर्न आदेश गर्न सक्नेछ।

(२) उपदफा (१) बमोजिमको विद्युतीय प्रणाली, सूचना वा उपकरण अदालत समक्ष पेश गर्नु सम्बन्धित व्यक्तिको कर्तब्य हुनेछ।

146. **<u>द्रुत संरक्षणः</u>** (१) कुनै विद्युतीय उपकरणमा भण्डारण गरिएको सूचना कुनै फौजदारी कसूरको अनुसन्धानको लागि आवश्यक रहेको र त्यस्तो सूचना नष्ट हुन सक्ने वा पहुँचवाट हटाईन सक्ने सम्भावना रहेको कुरामा अनुसन्धान अधिकृत विश्वस्त भएमा त्यस्तो विद्युतीय उपकरण वा सूचना नियन्त्रणमा रहेको व्यक्तिलाई लिखित सूचना दिई बढीमा सात दिन सम्म उक्त सूचनामा उल्लेख भए बमोजिमको सूचना सुरक्षित रहने प्रत्याभूत गर्न आदेश दिन वा त्यस्तो विद्युतीय उपकरण र सूचना यथास्थितिमा रहने व्यवस्था गर्न सक्नेछ।

(२) उपदफा (१) बमोजिमको आदेशको पालना गर्नु सम्बन्धित व्यक्तिको कर्तव्य हुनेछ।

147. **<u>ट्राफिक तथ्याङ्कमा पहुँच पु-याउन सक्ने:</u>** (१) कुनै खास सञ्चारसँग सम्बद्ध ट्राफिक तथ्याङ्क कुनै कसूरको अनुसन्धान प्रयोजनको लागि अदालतले तत्काल प्राप्त प्रमाणको आधारमा आवश्यक ठानेमा अनुसन्धान अधिकृतलाई खास संचार सम्बन्धी ट्राफिक तथ्याङ्कमा पहुँच राख्न अनुमति दिन सक्नेछ।

(२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि अनुसन्धानको क्रममा प्राप्त प्रमाण तथा सूचनाको आधारमा कुनै विद्युतीय उपकरण वा विद्युतीय उपकरणको प्रणालीमा भण्डारण भएका खास सूचना पीडितको जीवन रक्षाको लागी आवश्यक रहेको देखिएमा कम्तीमा प्रहरी निरीक्षक दर्जाको प्रहरी अधिकृतले आफूभन्दा एक तह माथिको अधिकृतको स्वीकृतिमा त्यस्तो प्रणालीसँगको खास संचारसँग सम्बन्धित ट्राफिक तथ्याङ्कमा पहुँच राख्न सक्नेछ।

148. **<u>ट्राफिक तथ्याङ्कको संकलन:</u>** (१) कुनै खास संचारसँग सम्बद्ध ट्राफिक तथ्याङ्क कुनै कसूरको अनुसन्धान प्रयोजनकोलागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक ठानेमा उक्त ट्राफिक तथ्याङ्कमा नियन्त्रण रहेको व्यक्तिलाई लिखित सूचना दिई देहाय बमोजिमको आदेश गर्न सक्नेछः-

(क) तोकिएको अवधिमा खास सञ्चारसँग सम्बद्ध ट्राफिक तथ्याङ्कको सञ्चार हुँदाहुँदैको अवस्था(रियल टाइम)मा संकलन वा अभिलेखन गर्न,

(ख) सम्बद्ध ट्राफिक तथ्याङ्कको सञ्चार हुँदाहुँदैको अवस्थामा संकलन वा अभिलेखन गर्न अनुसन्धान अधिकृतलाई अनुमति प्रदान गर्न वा सहयोग गर्न।

(२) कुनै खास संचारसँग सम्बद्ध ट्राफिक तथ्याङ्क कुनै कसूरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक ठानेमा अनुसन्धान अधिकृतलाई प्रविधिको प्रयोग गरी तोकिएको अवधिमा खास सञ्चारसँग सम्बद्ध ट्राफिक तथ्याङ्कको सञ्चार हुँदा हुँदैको अवस्थामा संकलन वा अभिलेखन गर्न अनुमति प्रदान गर्न सक्नेछ।

149. **<u>विषयवस्तुको अन्तरदोहन (इन्टरसेप्सन):</u>** (१) कुनै सञ्चारको विषयवस्तु कुनै कसूरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा न्यायाधिकरणले आवश्यक ठानेमा सेवा प्रदायकलाई प्रविधिको प्रयोग गरी विद्युतीय प्रणाली मार्फत प्रसार भएको खास सञ्चारको विषयवस्तु प्रसार हुँदाहुँदैको अवस्थामा संकलन वा अभिलेख गर्न वा अख्तियार प्राप्त अधिकारीलाई सोका लागि अनुमति दिन र सहायता गर्न आदेश गर्न सक्नेछ।

(२) कुनै सञ्चारको विषयवस्तु कुनै कसूरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक ठानेमा संचारको विषयवस्तु प्रसार हुँदाहुँदैको अवस्थामा संकलन वा अभिलेख गर्न अनुसन्धान अधिकृतलाई अख्तियारी प्रदान गर्न सक्नेछ।

150. **<u>डिजिटल विधि विज्ञानको प्रयोग</u>** (१) कुनै कसूरको अनुसन्धानमा यस परिच्छेदमा अन्यन्त्र उल्लेखित विधिले मात्र आवश्यक प्रमाण संकलन हुन सक्ने नदेखिएको अवस्थामा अनुसन्धान अधिकृतको विश्वसनीय आधार र अनुसन्धान गर्नु पर्ने देहाय बमोजिमको व्यहोरा सहितको निवेदनको आधारमा न्यायाधिकरणले डिजिटल विधि विज्ञान उपकरण तथा प्रणालीको प्रयोग गरी प्रमाण संकलन गर्न अनुमति दिन सक्नेछ।

(क) कसूरमा संदिग्ध व्यक्ति र निजको सेवा प्रदायकको नाम र ठेगाना,

(ख) परीक्षण गर्नुपर्ने विद्युतीय प्रणालीको विवरण,

(ग) परीक्षणको उपायको विवरण, औजार उपयोगको मात्रा र अवधि,

(घ) परीक्षण गर्नु पर्नाका आवश्यकताहरु,

(ङ) परीक्षण गरिने विद्युतीय प्रणाली र सोमा रहेको सूचना तथा तथ्याङ्कको सुरक्षाको सुनिश्चितता हुने व्यहोरा।

(२) उपदफा (१) बमोजिमको अनुमति एक पटकमा बढीमा तीन महिनाको लागि हुनेछ।

परिच्छेद-१७

सूचना प्रविधि न्यायाधिकरण सम्बन्धी व्यवस्था

151. न्यायाधिकरणको गठनः (१) नेपाल सरकारले राजपत्रमा सूचना प्रकाशन गरी परिच्छेद-१५ मा उल्लेख भए बमोजिमका कसूरहरुको शुरु कारवाही र किनारा गर्न दफा १५२ बमोजिमको योग्यता पुगेका व्यक्तिहरु मध्येबाट कानून सदस्य, सूचना प्रविधि सदस्य र वाणिज्य सदस्य भएको तीन सदस्यीय सूचना प्रविधि न्यायाधिकरणको गठन गर्नेछ।

(२) कानून सदस्य न्यायाधिकरणको अध्यक्ष हुनेछ।

(३) न्यायाधिकरणले आफ्नो अधिकारक्षेत्रको प्रयोग तोकिए बमोजिम गर्नेछ।

(४) नेपाल सरकारले न्यायाधिकरणको छुट्टै कार्यालय खोल्न सक्नेछ।

(५) न्यायाधिकरणले गरेको निर्णय वा आदेश उपर चित्त नबुझ्ने व्यक्तिले त्यस्तो आदेश वा निर्णय भएको मितिले पैतिस दिनभित्र सम्बन्धित उच्च अदालतमा पुनरावेदन गर्न सक्नेछ।

(६) यस दफामा अन्यत्र जुनसुकै कुरा लेखिएको भएता पनि उपदफा (१) बमोजिम न्यायधिकरण गठन नभएसम्मका लागि परिच्छेद-१५ मा उल्लेख भए बमोजिमका कसूरहरुको शुरु कारबाही र किनारा गर्ने क्षेत्राधिकार नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकिदिएको जिल्ला अदालतबाट हुनेछ।

152. न्यायधिकरणका सदस्यको योग्यताः (१) सूचना प्रविधि सम्बन्धी विषयमा ज्ञान भई जिल्ला अदालतको न्यायाधीश भइरहेको, भइसकेको वा हुन योग्यता पुगेको व्यक्ति न्यायाधिकरणको कानून सदस्य हुन योग्य हुनेछ।

(२) कम्प्युटर विज्ञान वा सूचना प्रविधि सम्बन्धी विषयमा कम्तीमा स्नातकोत्तर गरेको र सूचना प्रविधिको क्षेत्रमा कम्तीमा पन्ध्र वर्षको अनुभव प्राप्त नेपाली नागरिक न्यायाधिकरणको सूचना प्रविधि सदस्य हुन योग्य हुनेछ।

(३) सूचना प्रविधि सम्बन्धी विषयमा ज्ञान भई व्यवस्थापन वा वाणिज्यशास्त्रमा कम्तीमा स्नातकोत्तर गरी कम्तीमा पन्ध्र वर्षको अनुभव प्राप्त नेपाली नागरिक न्यायाधिकरणको वाणिज्य सदस्य हुन योग्य हुनेछ।

153. **<u>न्यायाधिकरणका सदस्यहरुको पदावधि, पारिश्रमिक र सेवाका शर्तः</u>** (१) न्यायाधिकरणमा नियुक्त अध्यक्ष तथा सदस्यको पदावधि पाँच वर्षको हुनेछ र निज पुनः नियुक्त हुन सक्नेछ।

(२) न्यायाधिकरणका नियुक्त अध्यक्ष तथा सदस्यको पारिश्रमिक, सुविधा र सेवाका अन्य शर्तहरु तोकिए बमोजिम हुनेछ।

(३) न्यायाधिकरणमा नियुक्त अध्यक्ष तथा प्रत्येक सदस्यले आफू नियुक्त भएपछि कार्यभार सम्हाल्नु अघि सम्बन्धित उच्च अदालतको मूख्य न्यायाधीश समक्ष आफ्नो पद तथा गोपनीयताको शपथ तोकिए बमोजिमको ढाँचामा लिनु पर्नेछ।

154. **<u>पद रिक्त हुने अवस्था र रिक्त पदको पूर्तिः</u>** (१) न्यायाधिकरणमा नियुक्त अध्यक्ष तथा सदस्यको पद देहायको कुनै अवस्थामा रिक्त हुनेछ :-

(क) निजको पदावधि समाप्त भएमा,

(ख) निज त्रिसठ्ठी वर्ष उमेर पूरा भएमा,

(ग) निजले राजीनामा दिएमा,

(घ) निज नैतिक पतन देखिने फौजदारी कसूरमा अदालतबाट दोषी ठहरिएमा, वा

(ङ) निजले आफ्नो पद अनुसारको आचरण नगरेको वा कर्तव्य पालना गर्न असक्षम भएको आरोपमा नेपाल सरकारले छानबिन गर्दा खराब आचरण गरेको वा आफ्नो कर्तव्य पालना गर्न असक्षम भएको प्रमाणित भएमा।

तर यस खण्ड बमोजिमको आरोप लगाइएको न्यायाधिकरणको सदस्यलाई सफाई पेश गर्ने मनासिब माफिकको मौका दिनु पर्नेछ।

(च) निजको मृत्यु भएमा,

(२) उपदफा (१) को खण्ड (ङ) मा जुनसुकै कुरा लेखिएको भए तापनि न्यायाधिकरणको कानून सदस्य बहालवाला न्यायाधीश भएमा प्रचलित कानून बमोजिम हुनेछ।

(३) उपदफा (१) को खण्ड (ङ) बमोजिमको प्रयोजनका लागि छानबिन गर्ने कार्यविधि तोकिए बमोजिम हुनेछ।

(४) उपदफा (१) बमोजिम न्यायाधिकरणको कुनै सदस्यको पद रिक्त हुन आएमा नेपाल सरकारले दफा १५३ बमोजिम योग्यता पुगेका व्यक्तिहरुमध्येबाट रिक्त पदको पूर्ति गर्नेछ।

155. **<u>न्यायाधिकरणका कर्मचारीः</u>** (१) न्यायाधिकरणलाई आफ्नो कार्य सम्पादन गर्न आवश्यक पर्ने कर्मचारी नेपाल सरकारले उपलब्ध गराउनेछ।

(२) न्यायाधिकरणको कर्मचारी सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

परिच्छेद- १८

विविध

156. **नियम बनाउने अधिकारः** (१) यस ऐनको कार्यान्वयन गर्न नेपाल सरकारले आवश्यक नियमहरू बनाउन सक्नेछ।

157. **अनुसूचीमा हेरफेर गर्न सक्नेः** नेपाल सरकारले समय समयमा नेपाल राजपत्रमा सूचना प्रकाशन गरी अनुसूचीमा हेरफेर गर्न सक्नेछ।

158. **बाधा अड्काउ फुकाउने अधिकारः** यस ऐनको कार्यान्वयन गर्न कुनै बाधा अड्काउ परेमा नेपाल सरकारले सो बाधा अड्काउ फुकाउनको लागि नेपाल राजपत्रमा सूचना प्रकाशन गरी आदेश जारी गर्न सक्नेछ।

159. **मुद्दा हेर्न बाधा नपर्ने** : यो ऐन प्रारम्भ हुनु अघि विद्युतीय कारोबार ऐन, २०६३ बमोजिमका मुद्दा हेर्न नेपाल सरकारले तोकेको जिल्ला अदालतमा विचाराधीन रहेका मुद्दा सोही जिल्ला अदालतले हेर्न यस ऐनले बाधा पुर्याएको मानिने छैन।

160. **खारेजी र बचाऊ** : (१) विद्युतीय कारोबार ऐन, २०६३ खारेज गरिएको छ।

(२) विद्युतीय कारोबार ऐन, २०६३ अनुसार भए-गरेका काम कारबाहीहरु यसै ऐन बमोजिम भए गरेको मानिनेछ।

अनुसूची-१
(दफा २ को खण्ड (त्र) सँग सम्बन्धित)

साइबर सुरक्षा सेवाहरु

(१)इन्फरमेशन सिस्टम अडिट
(२)साइबर सुरक्षासम्बन्धी कन्सल्टेशन
(३)सोसल इन्जिनियरिङ्ग अडिट
(४)साइबर सुरक्षा सम्बन्धी तालिम
(५)थ्रेट इन्टेलिजेन्स सम्बन्धी सेवा
(६)सेक्युरिटी अपरेसन सेन्टर व्यवस्थापन सम्बन्धी सेवा
(७)साइबर सुरक्षा जोखिम व्यवस्थापन सम्बन्धी सेवा
(८)साइबर सेक्युरिटी कम्प्लाइन्स मनिटरिङ्ग
(९)भल्नेरिबिलिटी एसेस्मेन्ट तथा पेनिट्रेस टेस्टिङ्ग
(१०)डाटाबेस सेक्युरिटी एसिस्मेन्ट
(११) नेटवर्क सेक्युरिटी टेस्टिङ्ग
(१२) एपलिकेसन सेक्युरिटी म्यानेजमेन्ट/टेस्टिङ्ग
(१३) नेटवर्क सेक्युरिटी म्यानेजमेन्ट/टेस्टिङ्ग
(१४) क्लाउड सेक्युरिटी म्यानेजमेन्ट/टेस्टिङ्ग
(१५) इन्टरनेट अफ थिँगस् सेक्युरिटी म्यानेजमेन्ट/टेस्टिङ्ग
(१६) डिजिटल फरेन्सिक
(१७) साइबर सेक्युरिटि इन्सिडेन्ट रेस्पोन्स