विधेयक संख्याः

सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा व्यवस्था गर्न बनेको विधेयक

संघीय संसद सचिवालय

संसद भवन

सिंहदरबार

उद्देश्य र कारण

विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ लाई समयसापेक्ष परिमार्जन गरी नयाँ प्रविधिअनुरूप बनाई साइबर सुरक्षा सम्बन्धी व्यवस्था थप गरी सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी विधेयक तर्जुमा गर्नु पर्ने आवश्यकता महसुस भएको छ ।

सूचना प्रविधिको विकास, प्रबर्द्धन तथा नियमन गर्न, विद्युतीय अभिलेख तथा डिजिटल हस्ताक्षरको सत्यता र विश्वसनीयता कायम राख्न, साइबर स्पेसमा रहेका सूचना, तथ्याङ्क वा विवरणको संरक्षण तथा व्यवस्थित प्रयोग गर्न र साइबर सुरक्षा सम्बन्धमा कानूनी व्यवस्था गर्न आवश्यक भएकोले **"सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा व्यवस्था गर्न बनेको विधेयक"** पेश गरेको छु।

१९ जेठ, २०८२
काठमाडौं ।

(पृथ्वीसुब्बा गुरुङ)
मन्त्री
सञ्चार तथा सूचना प्रविधि मन्त्रालय
सिंहदरवार, काठमाडौ

आर्थिक टिप्पणी

प्रस्तुत विधेयकको उद्देश्यअनुरूप सूचना प्रविधिको विकास, प्रबर्द्धन तथा नियमन गर्न, विद्युतीय अभिलेख तथा डिजिटल हस्ताक्षरको सत्यता र विश्वसनीयता कायम राख्न, साइबर स्पेसमा रहेका सूचना, तथ्याङ्क वा विवरणको संरक्षण तथा व्यवस्थित प्रयोग गर्नु पर्ने एवम् साइबर सुरक्षा केन्द्रलाई थप जिम्मेवारी र दायित्व पूरा गर्न सक्ने बनाउन यसको सुदृढीकरण गर्नु पर्ने भएकोले नेपाल सरकारलाई केही थप आर्थिक व्ययभार पर्ने देखिन्छ।

(पृथ्वीसुब्बा गुरुङ)
मन्त्री
सञ्चार तथा सूचना प्रविधि मन्त्रालय
सिंहदरवार, काठमाडौ

प्रत्यायोजित विधायन सम्बन्धी टिप्पणी

प्रस्तुत विधेयकमा रहेको प्रत्यायोजित विधायन सम्बन्धी टिप्पणी देहाय बमोजिम पेश गरिएको छः-

क्र.सं.	दफा	प्रत्यायोजित व्यवस्थापनको कारण	प्रत्यायोजित व्यवस्थापन अन्तर्गत बनाइने कानूनको प्रकृति र सीमा	प्रत्योजित व्यवस्थापनबाट पर्न सक्ने प्रभाव
१.	दफा १३	डिजिटल हस्ताक्षरको शुल्क निर्धारण गर्न आवश्यक भएको।	डिजिटल हस्ताक्षरको शुल्क निर्धारण नियमावलीमा गर्ने।	डिजिटल हस्ताक्षरको शुल्क निर्धारण भएको हुने ।
२.	दफा २० को उपदफा (२)	इजाजतपत्र नवीकरण दस्तुर निर्धारण गर्न आवश्यक भएको।	नवीकरण दस्तुरको निर्धारण नियमावलीमा गर्ने।	नवीकरण दस्तुर निर्धारण भएको हुने।
३.	दफा २१ को उपदफा (८)	प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्नको लागि नियन्त्रक समक्ष पेश गरेको कागजात, विवरण र वित्तीय तथा भौतिक स्रोतको जाँचबुझ गर्न आवश्यक भएको।	प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्नको लागि नियन्त्रक समक्ष पेश गरेको कागजात, विवरण र वित्तीय तथा भौतिक स्रोतको जाँचबुझ सम्बन्धी व्यवस्था नियमावलीमा गर्ने।	प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्नको लागि नियन्त्रक समक्ष पेश गरेको कागजात, विवरण र वित्तीय तथा भौतिक स्रोतको जाँचबुझ सम्बन्धी द्विविधा नरहने।
४.	दफा २४	डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र प्राप्त गर्न शुल्क र निवेदनको ढाँचा तोक्न आवश्यक भएको ।	डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र प्राप्त गर्न लाग्ने शुल्क र निवेदनको ढाँचाको निर्धारण नियमावलीले गर्ने।	डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र प्राप्त गर्न शुल्क र निवेदनको ढाँचा निर्धारण सम्बन्धी द्विविधा नरहने।
५.	दफा ४० को उपदफा (५)	डोमेन नामको नवीकरणको लागि शुल्क तोक्न आवश्यक भएको।	नवीकरण दस्तुर नियमावलीले तोक्ने।	नवीकरण दस्तुर तोकिने हुँदा सो सम्बन्धी द्विविधा नरहने।
६.	दफा ४४ को उपदफा (२)	डाटा सेन्टर वा क्लाउडमा कम्प्युटर प्रणाली राख्ने सम्बन्धी अन्य व्यवस्था तोक्न आवश्यक भएको।	डाटा सेन्टर वा क्लाउडमा कम्प्युटर प्रणाली राख्ने सम्बन्धी अन्य व्यवस्था नियमावलीले तोक्ने।	डाटा सेन्टर वा क्लाउडमा कम्प्युटर प्रणाली राख्ने सम्बन्धी व्यवस्था स्पष्ट हुने।
७.	दफा ५२ को उपदफा (३)	साइबर सुरक्षा सम्बन्धी सेवा प्रदान गरेको विवरणको अभिलेख राख्ने ढाँचा तोक्न आवश्यक	साइबर सुरक्षा सम्बन्धी सेवा प्रदान गरेको विवरणको अभिलेख राख्ने ढाँचा नियमावलीले तोक्ने।	साइबर सुरक्षा सम्बन्धी सेवा प्रदान गरेको विवरणको अभिलेख राख्ने

		भएको।		ढाँचा सम्बन्धी द्विविधा नरहने।
८.	दफा ५९ को उपदफा (५)	साइबर सुरक्षा परीक्षकको सूचीकरणका लागि आवश्यक योग्यता, मापदण्ड र कार्य तोक्न आवश्यक भएको।	साइबर सुरक्षा परीक्षकको सूचीकरणका लागि आवश्यक योग्यता, मापदण्ड र कार्य नियमावलीले तोक्ने।	साइबर सुरक्षा परीक्षकको सूचीकरणका लागि आवश्यक योग्यता, मापदण्ड र कार्य सम्बन्धी द्विविधा नरहने।
९.	दफा ६२ को उपदफा (४)	सूचना सुरक्षा सम्बन्धी अन्य व्यवस्था तोक्न आवश्यक भएको।	सूचना सुरक्षा सम्बन्धी अन्य व्यवस्था नियमावलीले तोक्ने।	सूचना सुरक्षा सम्बन्धी अन्य व्यवस्था स्पष्ट हुने।
१०.	दफा ६५	सेवा प्रदायकले सेवा प्रयोग गर्ने सूचना र अवधि तोक्न आवश्यक भएको।	सेवा प्रदायकले सेवा प्रयोग गर्ने सूचना र अवधि नियमावलीले तोक्ने।	सेवा प्रदायकले सेवा प्रयोग गर्ने सूचना र अवधि सम्बन्धी व्यवस्था स्पष्ट हुने।
११.	दफा ७८ को उपदफा (१)	सूचना प्रविधि सम्बन्धी तोकिए बमोजिमका उपकरणको हकमा स्वीकृत मापदण्डको आधारमा मात्र पैठारी तथा बिक्री वितरण गर्ने व्यवस्था गर्न आवश्यक भएको।	सूचना प्रविधि सम्बन्धी तोकिए बमोजिमका उपकरणको हकमा स्वीकृत मापदण्डको आधारमा मात्र पैठारी तथा बिक्री वितरण गर्ने व्यवस्था नियमावली र मापदण्डमा गर्ने।	सूचना प्रविधि सम्बन्धी उपकरणको पैठारी तथा बिक्री वितरण गर्ने सम्बन्धी व्यवस्था स्पष्ट हुने।
१२.	दफा ७८ को उपदफा (२)	उपकरणहरू र मापदण्ड, उपकरणको गुणस्तर, आयु र सुरक्षाको आधारमा स्वीकृत गर्ने प्रक्रिया तोक्न आवश्यक भएको।	उपकरणहरूको मापदण्ड, उपकरणको गुणस्तर, आयु र सुरक्षाको आधारमा स्वीकृत गर्ने प्रक्रिया सम्बन्धी व्यवस्था नियमवलीमा गर्ने।	उपकरणहरूको मापदण्ड, उपकरणको गुणस्तर, आयु र सुरक्षाको आधारमा स्वीकृत गर्ने प्रक्रिया सम्बन्धी द्विविधा नरहने।
१३.	दफा १११	यो ऐनको कार्यान्वयन गर्न नेपाल सरकारले आवश्यक नियम बनाउन सक्ने व्यवस्था गर्न आवश्यक भएको।	नेपाल सरकारले यस ऐनको उद्देश्य कार्यान्वयन गर्न आवश्यक पर्ने नियम बनाउने।	नेपाल सरकारले यस ऐनको उद्देश्य कार्यान्वयन गर्न आवश्यक पर्ने नियम बनाएको हुने।

नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी विधेयक तर्जुमा गर्न तयार पारिएको अवधारणापत्र

१. नयाँ ऐन बनाउनु पर्ने औचित्य र आवश्यकताः

विद्युतीय कारोवार तथा डिजिटल हस्ताक्षर सम्बन्धी प्रावधानलाई व्यवस्थित गर्ने समेतको उद्देश्यले विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ कार्यान्वयनमा रहेको छ । सूचना प्रविधिको विकास, प्रबर्द्धन र नियमन गर्न, विद्युतीय अभिलेख तथा डिजिटल 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 र यस क्षेत्रमा हुने अपराध नियन्त्रण गर्ने सम्बन्धमा आवश्यक कानूनी व्यवस्था गर्न मौजुदा विद्युतीय कारोबार ऐन, २०६३ लाई संशोधन र एकीकरण गर्न आवश्यक भएको छ। प्रस्तुत विधेयक तर्जुमा गर्नुपर्ने कारणहरू देहाय बमोजिम रहेका छन् :-

(क) संवैधानिक कारणः

(१) नेपालको संविधानको धारा ५१ को "राज्यका नीतिहरू" अन्तर्गत खण्ड (च) को विकास सम्वन्धी नीतिको उपखण्ड (५) र (७) मा उल्लिखित देहायका नीति कार्यान्वयन गर्न सहज हुनेछ ।

"(५) राष्ट्रिय आवश्यकता अनुसार सूचना प्रविधिको विकास र विस्तार गरी त्यसमा सर्वसाधारण जनताको सहज र सरल पहुँच सुनिश्चित गर्ने तथा राष्ट्रिय विकासमा सूचना प्रविधिको उच्चतम उपयोग गर्ने,

(७) एकीकृत राष्ट्रिय परिचय व्यवस्थापन सूचना प्रणाली विकास गरी नागरिकका सबै प्रकारका सूचना र विवरण एकीकृत रूपमा व्यवस्थापन गर्ने तथा यसलाई राज्यबाट उपलब्ध हुने सेवा सुविधा र राष्ट्रिय विकास योजनासँग आबद्ध गर्ने"

(२) धारा २८ बमोजिमको "गोपनियताको हक" लाई विद्युतीय माध्यममा समेत सुनिश्चित गर्न,

(३) धारा ४४ बमोजिमको "उपभोक्ताको हक" अन्तर्गत सूचना प्रविधिमा आधारित सेवा तथा व्यापारमा समेत सुनिश्चित गर्न ।

(ख) अन्तर्राष्ट्रिय दायित्वः

UN Resolution 72/200, Jan 2018

Increase the use of information and communications technologies to strengthen good governance.

Recognizes the critical importance of private sector investment in information and communications technology infrastructure, content and services and encourage Governments to create legal and regulatory frameworks conducive to increased investment and innovation.

(ग) सर्वोच्च अदालतको फैसलाः

(१) सम्मानीत सर्वोच्च अदालतबाट व्यक्तिगत विवरणको गोपनीयता र सूचना सुरक्षण सम्बन्धमा रिट नं. ०६९-WO-०२६८ को मुद्दामा मिति २०७२ माघ २१ गते निर्देशनात्मक आदेश जारी भएको।

(२) सर्वोच्च अदालतले नेपाली नागरिकको डाटा नेपाल सरकारको नियन्त्रणमा रहन तथा विदेशीको हातमा नजाने व्यवस्था मिलाउन मिति २०७४।०१।१० मा भएको

अन्तरिम आदेशलाई मिति २०७४।०१।२५ को आदेशले (०७३-WO-१०९७) निरन्तरता दिएकोले डाटाको सुरक्षा विषयको गाम्भिर्यता पुष्टि भएको।

(घ) सरकारको नीति तथा कार्यक्रमः

(१) साइबर सुरक्षा सम्बन्धी राष्ट्रिय नीति, २०८०

(२) सूचना तथा सञ्चार प्रविधि नीति, २०७२ को,-

(क) "११.१ सूचना तथा सञ्चार प्रविधिमा पहुँच माध्यम वा विषयवस्तु विकास" शिर्षक अन्तरगत निम्न नीति उल्लेख भएको छः-

- ❖ विकास एवं सार्वजनिक सेवा प्रवाह सम्वन्धी चुनौति सामना गर्न सूचना तथा प्रविधिमा आधारित नवीनतम तथा मौलिक प्रयोग प्रवर्द्धन गर्न विषेश कार्यक्रम (Innovative Use) लागु गरिनेछ ।

(ख) "११.६ सूचना तथा सञ्चार प्रविधि सम्बन्धी उद्योग क्षेत्रको विकास" शिर्षक अन्तरगत निम्न नीति उल्लेख भएको छः-

- ❖ अन्तर्राष्ट्रिय स्तरमा प्रतिस्पर्धा गर्न सक्ने सूचना तथा सञ्चार उद्योग क्षेत्रको विकास गर्न विशेष कार्यक्रम तर्जुमा गरी लागु गरिनेछ।सूचना तथा सञ्चार प्रविधिका क्षेत्रमा विदेशी श्रोत समेतको परिचालन गरी लागु गरिने परियोजनामा स्वदेशी व्यवसायीहरुलाई सहभागी हुने वातावरण निर्माण गरिनेछ ।

(ग) "११.१७ सुशासन तथा सार्वजनिक सेवा प्रवाहमा सूचना तथा सञ्चार प्रविधि" शिर्षक अन्तरगत निम्न नीति उल्लेख भएको छः-

- ❖ सूचना तथा सञ्चार प्रविधिको प्रयोगद्वारा सार्वजनिक सेवा प्रवाहलाई प्रभावकारी बनाउने विद्यमान प्रयासहरुलाई निरन्तरता दिइनेछ ।

(३) नेपाल सरकारको आ.व. २०८०/८१ को नीति तथा कार्यक्रममा देहाय वमोजिमका कार्यक्रमहरु रहेको छः

- ❖ सञ्चार तथा सूचना प्रविधिको प्रयोगमा आम नागरिकको पहुँच अभिवृद्धि गरिनेछ। शिक्षा स्वास्थ्य विकास निर्माण र सेवा प्रवाह लगायतका क्षेत्रमा सूचना प्रविधिको प्रयोगलाई विस्तार गरिनेछ। ज्ञानमा आधारित अर्थतन्त्रको विकास र सुशासनका लागि सूचना प्रविधि प्रणालीको अनुसन्धान, विकास र विस्तार गरिनेछ।
- ❖ सरकारी निकायबाट सञ्चालित अनलाइन प्रणालीहरुबीच अन्तरआबद्धता कायम गरी सेवा उपलब्ध गराइनेछ ।अनलाइन सेवाहरु वडा तहसम्म नै उपलब्ध गराइनेछ ।विद्युतीय प्रणालीबीच तथ्याङ्क आदन प्रदान गर्न डाटा एक्सचेन्ज प्लेटफर्म निर्माण गरिनेछ ।
- ❖ राष्ट्रिय साइबर सुरक्षा केन्द्र सञ्चालनमा ल्याई साइबर सुरक्षाजन्य जोखिमलाई न्यूनीकरण गरिनेछ।

(ङ) अन्य कुनै कारणः x

२. **नयाँ ऐन बनाई कार्यान्वयन भएपश्चात हासिल गरिने उपलब्धिः** नयाँ ऐन बनाई कार्यान्वयन भएपश्चात निम्न उपलब्धिहरू हासिल हुनेछनः-

(क) विद्युतीय शासनको अवधारणा प्रभावकारी रुपमा कार्यान्वयन गर्न कानूनी आधार तय हुने,
(ख) विद्युतीय अभिलेखले कानूनी मान्यता पाउने,
(ग) सूचना प्रविधि सम्बन्धी व्यवसायहरू व्यवस्थित, नियमित तथा मर्यादित भई यस क्षेत्रमा वैदेशिक लगानी वृद्दि हुने,
(घ) नेपालमा विद्युतीय स्वरुपमा रहेको सूचना सुरक्षा, संरक्षण तथा वैयक्तिक विवरणको गोपनीयताको स्तरमा उल्लेखनीय वृद्दि हुने ।

३. **प्रस्तावित विषयमा मौजुदा कानून भए** :

विद्युतीय कारोवार ऐन, २०६३ कार्यान्वयनमा रहेको तर विद्युतीय सरकार, सूचना प्रविधि सम्बन्धी उद्योग, व्यवसाय, सूचना सुरक्षा तथा संरक्षण, डोमेन नामको व्यवस्थापन, साइबर सुरक्षा, जनशक्ति, क्षमता विकास जस्ता महत्वपूर्ण विषय उक्त ऐनमा समेट्न सकिएको थिएन।

४. **मौजुदा कानून संशोधन गरी सो उपलब्धि हासिल हुन नसक्ने भए सो को कारणः**

(क) विद्युतीय सरकार, सूचना प्रविधि सम्बन्धि व्यवसाय, सूचना सुरक्षा तथा संरक्षण , डोमेन नामको व्यवस्थापन जस्ता महत्वपूर्ण विषय मौजुदा कानूनमा नसमेटिएकोले ती विषयहरुलाई समावेश गर्न जरुरी भएको,

(ख) विद्युतीय कारोवारले सूचना प्रविधिको एउटा पक्षलाई मात्र समेटेकोले सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी समग्र क्षेत्र तथा विषयवस्तुहरु समेट्न नसकेको,

(ग) कसुर तथा सजायको प्रावधानलाई समय अनुसार अझ व्यापक बनाई थप गर्नु पर्ने तथा कसुरको प्रकृति अनुसार फरक फरक निकायमा मुद्दा चलाउन मिल्ने गरी व्यवस्था गर्नु पर्ने भएको,

(घ) विद्युतीय कसुरको अनुसन्धान अभियोजन तथा प्रमाण संकलन तथा मुद्दा हेर्ने एवं पुनरावेदन सुन्ने सम्बन्धी प्रावधानहरु विस्तृत रुपमा समावेश गर्नु पर्ने भएको,

(ङ) नयाँ प्रविधिको विकास, विस्तार र परिवर्तनलाई सम्बोधन गर्नुपर्ने भएको ।

५. **प्रस्तावित विषयमा सरकारले कुनै विशेष नीति स्वीकृत गरेको भए उक्त नीति कुन विधि (Method) बाट तर्जुमा भएको हो ?**

- ❖ सूचना तथा सञ्चार प्रविधि नीति, २०७२ र साइबर सुरक्षा सम्बन्धी राष्ट्रिय नीति, २०८० स्वीकृत भएको र यी नीति मिश्रित पद्दति र बढोत्तरी पद्दतिबाट तर्जुमा भएका छन्।

६. **नीति निर्माणमा संलग्न प्रमुख पदाधिकारीः** नेपाल सरकार, सञ्चार तथा सूचना प्रविधि मन्त्रालय, नेपाल सरकारका सम्बद्ध अधिकारी र सरोकारवाला व्यक्ति, संघ तथा संस्थाको संलग्नता रहेको।

७. **प्रस्तुत विषयमा अन्य मुलुकमा कुनै कानून बनेको वा कुनै अन्तराष्ट्रिय संस्थाले नमूना कानून बनाएको भए त्यस्तो मुलुक र कानूनको नाम :**

(क) भारत (IT ACT 2000),

(ख) बङ्गलादेश (Information and Communication Technology (ICT) Act, 2006)

(ग) केन्या (Kenya Information and Communication Act, 1998)

८. **प्रस्तावित विषयमा कुनै निकायबाट अध्ययन तथा अनुसन्धान भई कानून निर्माण सम्बन्धमा कुनै सुझाब दिएको भए त्यसको संक्षिप्त व्यहोराः** मन्त्रालयमा विधेयकको मस्यौदा समिति बनाई अध्ययन कार्य भएको ।

९. **प्रस्तावित कानून कार्यान्वयन गर्न आर्थिक व्ययभार पर्ने भएमा अनुमानित वार्षिक व्ययभारः** हाल भइरहेका मन्त्रालय, विभाग, राष्ट्रिय साइबर सुरक्षा केन्द्र, प्रमाणीकरण नियन्त्रक लगायतका कार्यालयबाट काम हुने हुँदा कार्य विवरणको आधारमा केही व्ययभार मात्र थप हुने देखिन्छ।

१०. **प्रस्तावित कानून कार्यान्वयन गर्न थप संरचना आवश्यक पर्ने वा नपर्ने** : कार्य विवरणको आधारमा केही दरबन्दी र संरचना मात्र थप अवश्यक पर्ने देखिन्छ।

११. **प्रस्तावित कानून निर्माण गर्न कुनै निकायको परामर्श, सहमति लिनु पर्नेमा सो परामर्श वा सहमति प्राप्त भए वा नभएको** : मस्यौदा तर्जुमाको क्रममा विभिन्न मन्त्रालय, निकाय एवं सरोकारवाला व्यक्ति तथा संस्थासँग राय परामर्श लिइउको।

१२. **प्रस्तावित कानूनमा समावेश गर्न खोजिएका मुख्य विषय** :

(क) हालको विद्युतीय कारोबार ऐनमा रहेको विद्युतीय कारोवार तथा डिजिटल हस्ताक्षर सम्बन्धी प्रावधानलाई समयानुसार अध्यावधिक गरी समावेश गरिएको,

(ख) विद्युतीय शासन सम्बन्धी प्रावधानहरू,

(ग) डोमेन नाम दर्ता तथा व्यवस्थापन सम्बन्धी प्रावधान,

(घ) सूचना प्रविधि व्यवसाय सम्बन्धी प्रावधान,

(ङ) सूचना प्रविधिको क्षेत्रमा क्रियाशील जनशक्तिको क्षमता विकास सम्बन्धी व्यवस्था,

(च) सूचना सुरक्षा सम्बन्धी प्रावधान,

(छ) सेवा प्रदायक सम्बन्धी प्रावधान,

(ज) साइबर सुरक्षा केन्द्र सम्बन्धी व्यवस्था,

(झ) साइबर सुरक्षा परीक्षण र परीक्षक सम्बन्धी व्यवस्था,

(ञ) साइबर सुरक्षा सेवा प्रदान गर्न अनुमतिपत्र लिनुपर्ने व्यवस्था,

(ट) सूचना सुरक्षा सम्बन्धी व्यवस्था,

(ठ) हालको विद्युतीय कारोबार ऐनमा रहेको कसूर तथा सजाय, अनुसन्धान, अभियोजन, मुद्दा हेर्ने र पुनरावेदन सुन्ने सम्बन्धी समयसापेक्ष प्रावधान राखी कसुरको परिभाषालाई समेत थप स्पष्ट रुपमा व्याख्या गरिएको,

(ड) विद्युतीय कसुरको प्रमाण संकलन सम्बन्धी प्रावधानहरु थप गरिएको ।

सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा व्यवस्था गर्न बनेको विधेयक

प्रस्तावनाः सूचना प्रविधिको विकास, प्रबर्द्धन तथा नियमन गर्न, विद्युतीय अभिलेख तथा डिजिटल हस्ताक्षरको सत्यता र विश्वसनीयता कायम राख्न, साइबर स्पेसमा रहेका सूचना, तथ्याङ्क वा विवरणको संरक्षण तथा व्यवस्थित प्रयोग गर्न र साइबर सुरक्षा सम्बन्धी प्रचलित कानूनलाई संशोधन र एकीकरण गर्न वाञ्छनीय भएकोले,

सङ्घीय संसदले यो ऐन बनाएको छ।

परिच्छेद-१

प्रारम्भिक

१. **संक्षिप्त नाम, प्रारम्भ र विस्तारः** (१) यस ऐनको नाम "सूचना प्रविधि तथा साइबर सुरक्षा ऐन, २०८२" रहेको छ।

(२) यो ऐन तुरुन्त प्रारम्भ हुनेछ।

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

२. **परिभाषाः** विषय वा प्रसङ्गले अर्को अर्थ नलागेमा यस ऐनमा,-

(क) "अनुसन्धान अधिकृत" भन्नाले दफा १०४ बमोजिमको अनुसन्धान अधिकृत सम्झनु पर्छ।

(ख) "उत्पत्तिकर्ता" भन्नाले विद्युतीय अभिलेख तयार गर्ने, भण्डारण गर्ने वा सम्प्रेषण गर्ने व्यक्ति सम्झनु पर्छ र सो शब्दले त्यस्तो कार्य गर्न लगाउने अन्य व्यक्तिलाई समेत जनाउँछ।

(ग) "कम्प्युटर" भन्नाले विद्युतीय स्वरुपको तथ्याङ्क वा विवरणको उत्पादन, प्रशोधन तथा भण्डारण गर्न सकिने कुनै पनि विद्युतीय उपकरण सम्झनु पर्छ।

(घ) "कम्प्युटर प्रणाली" भन्नाले आगत र निर्गत (इन्पुट र आउटपुट) सहायता संयन्त्र लगायतका कम्प्युटर कार्यक्रम, विद्युतीय निर्देशन, आगत र निर्गत तथ्याङ्क समाविष्ट भएको र तार्किक, अङ्क गणितीय, तथ्याङ्क सञ्चय तथा पुनःप्राप्ति, सञ्चार र नियन्त्रण लगायतका कार्यसम्पादन गर्ने संयन्त्र वा संयन्त्रको समूह सम्झनु पर्छ।

(ङ) "कम्प्युटर प्रोग्राम" भन्नाले तथ्याङ्क वा विवरण प्रशोधन गर्न निर्देशन दिने वा कम्प्युटरको माध्यमबाट कुनै निश्चित कार्य गर्न सकिने कुनै विद्युतीय आदेश वा आदेशको समूह सम्झनु पर्छ।

(च) "केन्द्र" भन्नाले दफा ४६ बमोजिमको राष्ट्रिय साइबर सुरक्षा केन्द्र सम्झनु पर्छ।

(छ) “क्लाउड सेवा" भन्नाले क्लाउड कम्प्युटिङ्ग सेवा प्रदायकबाट प्रयोगकर्ताको माग बमोजिम इन्टरनेटको माध्यमबाट प्राप्त हुने सूचना प्रविधिसँग सम्बन्धित सफ्टवेयर र पूर्वाधार लगायतका सेवा सम्झनु पर्छ।

(ज) “जोडी साँचो (की पीयर)” भन्नाले डिजिटल हस्ताक्षर सिर्जना गर्ने निजी साँचो र सो हस्ताक्षर सम्पुष्टि गर्ने गणितीय रुपमा अन्तरआबद्ध गरिएको सार्वजनिक साँचोको जोडी सम्झनु पर्छ।

(झ) "ट्राफिक तथ्याङ्क" भन्नाले इलेक्ट्रोनिक सञ्चार नेटवर्कमा प्रसारण गरिएको कुनै डाटा र उक्त डाटा सञ्चारको मार्ग, अवधि वा समय लगायत सोसँग सम्बन्धित तथ्याङ्क सम्झनु पर्छ।

(ञ) “डाटा” भन्नाले कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कमा प्रयोग गर्ने उद्देश्यले अक्षर, अङ्क, छवि, ध्वनि वा श्रव्य दृश्यमा औपचारिक तवरले तयार गरिएको वा कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कद्वारा उत्पादन गरिएको सूचना वा विवरण सम्झनु पर्छ।

(ट) “डाटा सेन्टर” भन्नाले डाटा भण्डारण, व्यवस्थापन, प्रशोधन वा आदानप्रदान गर्नको लागि व्यवस्था गरिएको उच्च क्षमताको कम्प्युटर पूर्वाधार सम्झनु पर्छ र सो शब्दले सर्भर, राउटर, स्वीच, फायरवाल, स्टोरेज र अग्नि नियन्त्रण प्रणाली, वातानुकूलित व्यवस्थापन प्रणाली सहितको सुविधा रहेको संरचनालाई समेत जनाउँछ।

(ठ) “डिजिटल हस्ताक्षर” भन्नाले दफा १० को उपदफा (२) बमोजिमको सर्त पूरा भएको विद्युतीय स्वरुपको हस्ताक्षर सम्झनु पर्छ।

(ड) "डोमेन नाम" भन्नाले इन्टरनेटको माध्यमबाट वेब साइटमा पहुँच पुऱ्याउनको लागि प्रदान गरिने वेबसाइटको ठेगाना 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 सिर्जना गर्न प्रयोग गरिएको जोडी साँचोमध्ये सम्बन्धित प्रयोगकर्तासँग मात्र रहने साँचो सम्झनु पर्छ।

(त) “निर्देशक समिति” भन्नाले दफा ६६ बमोजिमको सूचना प्रविधि तथा साइबर सुरक्षा निर्देशक समिति सम्झनु पर्छ।

(थ) “नियन्त्रक” भन्नाले दफा १४ बमोजिम तोकिएको नियन्त्रक सम्झनु पर्छ।

(द) “पहुँच (एक्सेस)" भन्नाले कुनै कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कको तार्किक,अङ्क गणितीय वा स्मरण सम्पदा (मेमोरी रिसोर्स) मा प्रवेश प्राप्त गर्ने, त्यस्ता सम्पदालाई निर्देशन दिने वा त्यस्ता सम्पदासँग सञ्चार सम्पर्क गर्न सक्ने अवसर सम्झनु पर्छ।

(ध) “प्रमाणपत्र” भन्नाले दफा २५ बमोजिम प्रमाणीकरण निकायले जारी गरेको डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र सम्झनु पर्छ।

(न) “प्रमाणीकरण निकाय” भन्नाले दफा १६ बमोजिम इजाजतपत्र प्राप्त वा मन्त्रालयले तोकेको प्रमाणीकरण निकाय सम्झनु पर्छ।

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

(फ) "प्रापक" भन्नाले उत्पत्तिकर्ताको चाहाना अनुरुप सम्प्रेषण गरिएका विद्युतीय अभिलेख प्राप्त गर्ने मध्यस्थकर्ता (इन्टरमिडीयरी) बाहेकका व्यक्ति सम्झनु पर्छ।

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

(भ) “विभाग” भन्नाले नेपाल सरकारको सूचना प्रविधि सम्बन्धी विषय हेर्ने विभाग सम्झनु पर्छ।

(म) “विद्युतीय अभिलेख” भन्नाले कम्युटर वा कम्प्युटर प्रणालीको प्रयोगबाट सिर्जना गरी सम्प्रेषण, प्राप्त वा जम्मा गरिएको सूचना, तथ्याङ्क, विवरण वा अभिलेखको लिखित, मुद्रित, श्रव्य, दृष्य वा श्रव्यदृष्य लगायतका विद्युतीय स्वरुपमा रहेका सबै किसिमका अभिलेख सम्झनु पर्छ।

(य) “विद्युतीय प्रणाली” भन्नाले अन्तरआवद्ध वा आपसमा सम्बन्धित विद्युतीय उपकरण वा उपकरणको समूह सम्झनु पर्छ र सो शब्दले एक वा एक भन्दा बढी उपकरणको माध्यमबाट विद्युतीय तथ्याङ्क वा सिग्नलको स्वचालित रुपमा प्रशोधन (अटोमेटिक प्रोसेसिङ्ग) गर्ने कार्य तथा स्थायी वा अस्थायी रुपमा विद्युतीय भण्डारण गर्ने कार्यलाई समेत जनाउँछ।

(र) "वैयक्तिक विवरण" भन्नाले कुनै व्यक्तिको देहायको विषयसँग सम्बन्धित सूचना वा विवरण सम्झनु पर्छः-

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

(२) निजको शैक्षिक उपाधि,

(३) निजको औंलाको छाप, हस्तरेखा, आँखाको रेटिना, रगत समूह वा निजको अन्य जैविक विवरण,

(४) निजको ठेगाना, टेलिफोन वा इमेल वा अन्य कुनै विद्युतीय पहिचान,

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

(ल) "सफ्टवेयर" भन्नाले कम्प्युटर वा इलेक्ट्रोनिक उपकरण प्रयोग गरी डाटा प्रोसेस गर्ने तथा कम्प्युटर हार्डवेयर सञ्चालन गर्ने क्षमता भएको सिष्टम, सफ्टवेयर र एप्लिकेशन सफ्टवेयर जस्ता कम्प्युटर प्रणालीको कुनै खास अंश सम्झनु पर्छ।

(व) "सरकारी निकाय" भन्नाले नेपाल सरकारको मन्त्रालय, सचिवालय वा सो अन्तर्गतका कार्यालय, संवैधानिक निकाय, अदालत, प्रदेश सरकार वा स्थानीय तह र सो अन्तर्गतको कार्यालय सम्झनु पर्छ र सो शब्दले यस्तै प्रकृतिका अन्य सरकारी कार्यालयलाई समेत जनाउँछ।

(श) "साइबर सुरक्षा" भन्नाले कम्प्युटर वा कम्प्युटर प्रणालीमा भण्डारण वा प्रसारण हुने विद्युतीय अभिलेख वा सामग्रीको गोपनीयता र अखण्डता कायम गरी सुरक्षित राख्ने तथा कम्प्युटर वा कम्प्युटर प्रणालीमा अनधिकृत पहुँच वा साइबर आक्रमणबाट सुरक्षित राख्न अपनाइने सुरक्षा प्रणाली सम्झनु पर्छ।

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

(स) "साइबर सुरक्षा जोखिम" भन्नाले कम्प्युटर प्रणालीमा रहेको कमजोरी वा अन्य कुनै कारणले कम्प्युटर प्रणाली मार्फत साइबर सुरक्षामा पर्न सक्ने अनधिकृत पहुँच सम्झनु पर्छ।

(ह) “साइबर सुरक्षा सेवा प्रदायक” भन्नाले दफा ५० बमोजिमको साइबर सुरक्षा सेवा प्रदान गर्न केन्द्रमा सूचीकृत भएको व्यक्ति वा संस्था सम्झनु पर्छ।

(क्ष) “साइबर स्पेस” भन्नाले कम्प्युटर वा इन्टरनेटको प्रयोग गरी सूचना प्रविधि सम्बन्धी पूर्वाधार तथा कम्प्युटर प्रणालीबिच सूचनाको आदानप्रदान हुन सक्ने गरी विश्वव्यापी अन्तरसम्बन्धित सञ्जाल कायम रहने भर्चुअल क्षेत्र सम्झनु पर्छ।

(त्र) “सार्वजनिक संस्था” भन्नाले देहायका संस्था सम्झनु पर्छः-

(१) नेपाल सरकार, प्रदेश सरकार वा स्थानीय तह अन्तर्गतका सरकारी निकाय,

(२) प्रचलित कानून बमोजिम नेपाल सरकार वा प्रदेश सरकारद्वारा स्थापित आयोग, समिति, संस्थान, प्राधिकरण, निगम, प्रतिष्ठान, बोर्ड, केन्द्र, परिषद् र यस्तै प्रकृतिका अन्य सङ्गठित संस्था,

(३) नेपाल सरकार वा प्रदेश सरकारको पूर्ण वा आंशिक स्वामित्व वा नियन्त्रणमा रहेको संस्था, कम्पनी वा समिति,

(४) नेपाल सरकार वा प्रदेश सरकारद्वारा सञ्चालित वा नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहको पूर्ण वा आंशिक अनुदानप्राप्त विश्वविद्यालय, महाविद्यालय, विद्यालय, अनुसन्धान केन्द्र र अन्य यस्तै प्राज्ञिक वा शैक्षिक संस्था,

(५) नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहको ऋण, अनुदानबाट सञ्चालित वा जमानतप्राप्त संस्था,

(६) उपखण्ड (२), (३), (४) वा (५) मा उल्लिखित संस्थाको पूर्ण वा आंशिक स्वामित्व भएको वा नियन्त्रण रहेको संस्था,

(७) नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहको अनुमति वा सम्झौता बमोजिम प्राकृतिक स्रोत साधनको संरक्षण, सम्बर्द्धन, उपयोग वा उपभोग गर्न वा विकास निर्माण सम्बन्धी काम गर्न गठित उपभोक्ता समिति वा यस्तै प्रकारका अन्य संस्था,

(८) नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी सार्वजनिक संस्था भनी तोकेको अन्य कुनै संस्था।

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

(कक) “सूचना” भन्नाले सरकारी निकाय वा सार्वजनिक संस्था वा कुनै व्यक्तिबाट सम्पादन हुने वा भएको महत्त्वपूर्ण काम, कारबाही वा निर्णयसँग सम्बन्धित कुनै तथ्याङ्क वा विवरण सम्झनु पर्छ।

(कख) “सूचना प्रविधि” भन्नाले कम्युटर वा कम्प्युटर प्रणालीको प्रयोग गरिएका सबै स्वरुपका सूचना सिर्जना गर्ने, उत्पादन गर्ने, सम्प्रेषण गर्ने, प्राप्त गर्ने वा सुरक्षण गर्ने प्रविधि सम्झनु पर्छ।

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

(कघ) “सेवा प्रदायक” भन्नाले कुनै तेस्रो पक्षसँगको सम्झौता बमोजिम सूचना आदानप्रदान वा भण्डारण गर्ने डाटा सेन्टर, क्लाउड सेवा वा सोही प्रकृतिको अन्य सेवा प्रदायक सम्झनु पर्छ ।

(कङ) “संवेदनशील सूचना पूर्वाधार” भन्नाले दफा ५४ बमोजिम तोकिएको संवेदनशील सूचना पूर्वाधार सम्झनु पर्छ।

(कच) “संवेदनशील सूचना पूर्वाधारको धनी” भन्नाले संवेदनशील सूचना पूर्वाधारको स्वामित्व प्राप्त सरकारी निकाय, सार्वजनिक संस्था वा व्यक्ति सम्झनु पर्छ।

परिच्छेद-२

विद्युतीय अभिलेख

३. **विद्युतीय अभिलेखले कानूनी मान्यता पाउने:** यो ऐन वा यस ऐन अन्तर्गत बनेको नियममा उल्लिखित प्रक्रिया पूरा गरी प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेखको लिखित, मुद्रित वा अन्य कुनै स्वरुपमा हुनु पर्ने भनी उल्लेख गरिएको विषय विद्युतीय स्वरुपमा अभिलेख राख्न सकिनेछ र त्यस्तो विद्युतीय अभिलेखले कानूनी मान्यता प्राप्त गर्नेछ।

४. **सुरक्षित राख्नु पर्ने**: (१) प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेख कुनै खास अवधिसम्म सुरक्षित राख्नु पर्ने भनी उल्लेख गरिएकोमा त्यस्तो सूचना, लिखत, तथ्याङ्क वा अभिलेख विद्युतीय स्वरुपमा पनि सोही अवधिसम्म सुरक्षित राख्नु पर्नेछ ।

(२) उपदफा (१) बमोजिमको सुरक्षित राखिएको विद्युतीय अभिलेखले देहायका सर्त पूरा गरेमा 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, र

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

५. **मूल वा सक्कल अभिलेखको रुपमा पेश गर्न सकिने**: (१) प्रचलित कानूनमा मूल वा सक्कल अभिलेख नै पेश गर्नु पर्ने वा सुरक्षित राख्नु पर्ने भनी उल्लेख गरिएकोमा देहाय बमोजिमका सर्त पूरा भएमा त्यस्तो मूल वा सक्कल अभिलेखको विद्युतीय प्रति पेश गर्न सकिनेछः-

(क) विद्युतीय स्वरुपमा सिर्जना गरिएको समयदेखि सो अभिलेखमा कुनै पनि किसिमबाट परिवर्तन गरिएको छैन भनी विश्वास गर्न सकिने 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।

६. **सुरक्षित विद्युतीय अभिलेख मानिने** : सुरक्षण कार्यविधि अपनाई सिर्जना गरिएको विद्युतीय अभिलेख तोकिए बमोजिम परीक्षण गर्दा कुनै किसिमको हेरफेर गरिएको छैन भन्ने यकिन भएमा त्यस्तो विद्युतीय अभिलेखलाई सुरक्षित विद्युतीय अभिलेख मानिनेछ।

७. **उत्पत्तिकर्ताको अभिलेख मानिने**: (१) देहायका अवस्थामा कुनै विद्युतीय अभिलेख उत्पत्तिकर्ताको अभिलेख मानिनेछः-

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

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

(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 आधारमा तत्सम्बन्धी कार्य गर्ने अधिकार प्राप्त गर्नेछ।

८. **विद्युतीय अभिलेखको प्राप्ति र स्वीकार गर्ने प्रक्रिया**: (१) उत्पत्तिकर्ताले विद्युतीय अभिलेख पठाउँदाका बखत वा पठाउनुभन्दा अगावै प्रापकलाई सो विद्युतीय अभिलेख प्राप्त भएको सूचना वा जानकारी पठाउन अनुरोध गरेको वा त्यसरी सूचना वा जानकारी पठाउन उत्पत्तिकर्ता र प्रापकको बिचमा सहमति भएको अवस्थामा त्यस्तो विद्युतीय अभिलेखको प्राप्ति स्वीकार गर्ने सम्बन्धमा उपदफा (२), (३) र (४) का व्यवस्था लागू हुनेछन्।

(२) विद्युतीय अभिलेख प्राप्त भएको सूचना वा जानकारी कुनै खास ढाँचामा वा कुनै खास तरिकाबाट दिनु पर्ने गरी उत्पत्तिकर्ता र प्रापकबिचमा कुनै सम्झौता नभएको अवस्थामा त्यस्तो सूचना वा जानकारी 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) उत्पत्तिकर्ता र प्रापकको बीचमा कुनै विद्युतीय अभिलेखको सम्बन्धमा त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्रापकबाट प्राप्त गरेपछि मात्र निजको हकमा बन्धनकारी हुने भनी सहमति भएकोमा त्यस्तो सूचना वा भरपाई प्राप्त नभएसम्म प्रापकको हकमा बन्धनकारी 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 उत्पत्तिकर्ता वा प्रापकबिच कुनै समय निर्धारण वा मञ्जुरी नभएको भए तोकिए बमोजिमको समयभित्र उत्पत्तिकर्ताले प्रापकबाट त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्राप्त गरिसकेको मानिनेछ।

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

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

(३) उत्पत्तिकर्ता र प्रापकबिचमा अन्यथा सम्झौता भएकोमा बाहेक कुनै विद्युतीय अभिलेखलाई उत्पत्तिकर्ताको व्यवसाय सञ्चालन हुने स्थानबाट सम्प्रेषण गरेको र प्रापकको व्यवसाय सञ्चालन हुने स्थानमा प्राप्त भएको मानिनेछ।

<u>स्पष्टीकरण:</u> यस उपदफाको प्रयोजनको लागि "व्यवसाय सञ्चालन हुने स्थान" भन्नाले,-

(क) उत्पत्तिकर्ता वा प्रापकको एकभन्दा बढी व्यवसाय सञ्चालन हुने स्थान रहेको अवस्थामा सम्बन्धित कारोबारसँग सम्बद्ध रहेको व्यवसाय सञ्चालन हुने स्थान सम्झनु पर्छ।

(ख) उत्पत्तिकर्ता वा प्रापकको कुनै व्यवसाय सञ्चालन हुने स्थान नभएको अवस्थामा निजको बसोबासको स्थानलाई नै निजको व्यवसाय सञ्चालन हुने स्थान सम्झनु पर्छ।

परिच्छेद-३

<u>डिजिटल हस्ताक्षर, नियन्त्रक र प्रमाणीकरण निकाय</u>

१०. **<u>डिजिटल हस्ताक्षर</u>**: (१) प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेखलाई हस्ताक्षरबाट प्रमाणित गर्नु पर्ने भएमा त्यस्तो काम डिजिटल हस्ताक्षरबाट गर्न सकिनेछ।

(२) उपदफा (१) को प्रयोजनको लागि डिजिटल हस्ताक्षरको सिर्जना गर्न देहायको सर्त 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, र

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

११. **<u>डिजिटल हस्ताक्षरको कानूनी मान्यता</u>** : प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेखलाई हस्ताक्षरद्वारा प्रमाणित गर्नु पर्ने वा कुनै लिखतमा कुनै व्यक्तिको हस्ताक्षर गरिएको हुनु पर्ने भनी उल्लेख गरिएको रहेछ भने त्यस्ता सूचना, लिखत, तथ्याङ्क 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।

१२. **सुरक्षित डिजिटल हस्ताक्षर मानिने**: यस ऐन बमोजिम सुरक्षण कार्यविधि अपनाई परीक्षण र सम्पुष्टि गरिएको कुनै विद्युतीय अभिलेखमा रहेको डिजिटल हस्ताक्षरलाई सुरक्षित डिजिटल हस्ताक्षर मानिनेछ।

१३. **डिजिटल हस्ताक्षरको शुल्क निर्धारण:** प्रमाणीकरण निकायले डिजिटल हस्ताक्षर सम्बन्धी सेवा उपलब्ध गराए बापत प्रयोगकर्तासँग लिने शुल्क सम्बन्धी व्यवस्था तोकिए बमोजिम हुनेछ।

१४. **नियन्त्रक तोक्ने**: (१) इजाजतपत्र जारी गर्ने, सो सम्बन्धमा आवश्यक समन्वय तथा नियमन गर्ने प्रयोजनको लागि एक नियन्त्रकको कार्यालय रहनेछ।

(२) नियन्त्रकको कार्यालयको प्रमुखको रुपमा काम गर्न नेपाल सरकारले निजामती सेवाको कुनै सेवा/समूहको राजपत्राङ्कित प्रथम श्रेणीको अधिकृतलाई नियन्त्रक तोक्नेछ।

(३) यो ऐन प्रारम्भ हुँदाको बखत कायम रहेको नियन्त्रकको कार्यालय यसै ऐन बमोजिम स्थापना भएको नियन्त्रक कार्यालय मानिनेछ।

१५. **नियन्त्रकको काम, कर्तव्य र अधिकार**: यस ऐनमा अन्यत्र उल्लिखित काम, कर्तव्य र अधिकारको अतिरिक्त नियन्त्रकको प्रमाणीकरण निकाय सम्बन्धी काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) इजाजतपत्र प्रदान गर्ने,

(ख) इजाजतपत्र निलम्बन गर्ने वा रद्द गर्ने,

(ग) काम कारबाहीको सुपरिवेक्षण तथा रेखदेख गर्ने र आवश्यकता अनुसार निर्देशन दिने,

(घ) डिजिटल हस्ताक्षरको सम्पुष्टि गर्ने सम्बन्धमा कायम गर्नु पर्ने स्तर निर्धारण गर्ने,

(ङ) आफ्नो कारोबार सञ्चालन गर्दा पालन गर्नु पर्ने सर्त निर्धारण गर्ने,

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

(छ) यस परिच्छेद बमोजिम प्रकट गरेका सूचनाको अभिलेख खडा गरी सार्वजनिक रुपमा पहुँचयोग्य हुने गरी तथ्याङ्कको व्यवस्था गर्ने र सो तथ्याङ्कलाई अद्यावधिक गर्ने,

(ज) वार्षिक कार्यसम्पादन परीक्षण गर्ने, गराउने, र

(झ) डिजिटल हस्ताक्षरको प्रमाणपत्र सम्बन्धी कार्य गर्ने ।

१६. **प्रमाणीकरण निकायले इजाजतपत्र लिनुपर्ने:** (१) डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्ने, निलम्बन वा रद्द गर्ने काम समेतको लागि प्रमाणीकरण निकायले यस ऐन बमोजिम इजाजतपत्र लिनु पर्नेछ।

(२) उपदफा (१) बमोजिमको इजाजतपत्र प्राप्त नगरी कसैले पनि प्रमाणीकरण निकायको रुपमा कार्य गर्न वा गराउन हुँदैन।

(३) उपदफा (१) र (२) मा जुनसुकै कुरा लेखिएको भए तापनि नियन्त्रकको कार्यालयमा सूचीकृत हुने गरी मन्त्रालयले कुनै सरकारी निकायलाई प्रमाणीकरण निकायको रुपमा काम गर्न तोक्न सक्नेछ।

(४) उपदफा (३) बमोजिम तोकिएको निकायले सरकारी निकायको लागि डिजिटल हस्ताक्षरको प्रमाणपत्र जारी गर्न, निलम्बन वा रद्द गर्न सक्नेछ।

(५) उपदफा (२) बमोजिम इजाजतपत्र प्राप्त नगरी प्रमाणीकरण निकायको रुपमा कार्य गर्ने वा गराउनेलाई नियन्त्रकले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।

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

(२) उपदफा (१) बमोजिम मान्यता प्राप्त प्रमाणीकरण गर्ने निकायको नेपालमा शाखा कार्यालय रहेको हुनु पर्नेछ।

१८. **इजाजतपत्रको लागि निवेदन दिनु पर्ने:** (१) दफा १६ बमोजिम प्रमाणीकरण निकायको रुपमा काम गर्न तोकिए बमोजिमको योग्यता पुगेका व्यक्तिले तोकिए बमोजिमको दस्तुर सहित इजाजतपत्र प्राप्त गर्न देहाय बमोजिमका कागजात संलग्न गरी नियन्त्रक समक्ष निवेदन दिनु पर्नेछ :-

(क) प्रमाणीकरण सम्बन्धी विवरण,

(ख) निवेदकको पहिचान तथा सनाखतको पुष्टि हुने कागजात,

(ग) जनशक्ति, वित्तीय तथा भौतिक स्रोत खुल्ने कागजात।

(२) दफा १६ को उपदफा (३) बमोजिमको सरकारी निकायलाई उपदफा (१) को खण्ड (ग) बमोजिमको कागजात र इजाजतपत्र दस्तुर आवश्यक पर्ने छैन।

१९. **इजाजतपत्र दिनु पर्ने:** (१) दफा १८ बमोजिम इजाजतपत्रको लागि प्राप्त निवेदन उपर जाँचबुझ गर्दा उपयुक्त देखिएमा नियन्त्रकले तोकिएको ढाँचामा इजाजतपत्र दिनु पर्नेछ।

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

२०. **इजाजतपत्र नवीकरण गर्नु पर्ने**: (१) प्रमाणीकरण निकायले प्राप्त गरेको इजाजतपत्र प्रत्येक दुई वर्षमा नवीकरण गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिम इजाजतपत्रको नवीकरण गर्न चाहने प्रमाणीकरण निकायले 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 आवश्यक जाँचबुझ गरी इजाजतपत्रको अवधि समाप्त हुनुभन्दा एक महिना अघि निर्णय गरिसक्नु पर्नेछ।

(४) उपदफा (३) बमोजिम नवीकरण सम्बन्धी जाँचबुझ तथा निर्णय गर्दा दफा २९ बमोजिमको कार्यसम्पादन परीक्षण प्रतिवेदन समेतलाई आधारको रुपमा लिन सकिनेछ।

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

(६) उपदफा (१) बमोजिम नवीकरण नगरी प्रमाणीकरण निकायको रुपमा काम गर्ने व्यक्ति वा संस्थालाई नियन्त्रकले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।

२१. **जाँचबुझ तथा इजाजतपत्र निलम्बन गर्न सक्ने**: (१) प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्नको लागि नियन्त्रक समक्ष पेश गरेको कागजात, विवरण र वित्तीय तथा भौतिक स्रोत झुट्ठा भएमा वा कारोबार सञ्चालन गर्दा पालन गर्नु पर्ने सर्तको पालना नगरेमा वा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको उल्लङ्घन गरेको शंका गर्नुपर्ने मनासिव कारण देखिएमा नियन्त्रक आफैंले जाँचबुझ गर्न वा अन्य कुनै अधिकृत कर्मचारीद्वारा आवश्यक जाँचबुझ गराउन सक्नेछ।

(२) उपदफा (१) बमोजिम जाँचबुझ पूरा नभएसम्मका लागि नियन्त्रकले प्रमाणीकरण निकायको इजाजतपत्र निलम्बन गर्न सक्नेछ।

(३) उपदफा (२) बमोजिम निलम्बनमा परेको प्रमाणीकरण निकाय एक मात्र इजाजतपत्रवाला भएमा त्यसरी निलम्बनमा परेको अवधिभर सो सम्बन्धी काम नियन्त्रकको कार्यालयले गर्नेछ।

(४) उपदफा (२) बमोजिम निलम्बनमा परेको प्रमाणीकरण निकायले प्रमाणीकरण कार्यमा प्रयोग गरेका हार्डवेयर, सफ्टवेयर, सूचना प्रविधि प्रणाली र सोसँग सम्बन्धित तथ्याङ्क नियन्त्रकलाई बुझाउनु पर्नेछ।

(५) उपदफा (१) बमोजिम जाँचबुझ गर्दा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको पालना भएको नदेखिएमा नियन्त्रकले त्यस्तो प्रमाणीकरण निकायलाई आवश्यक निर्देशन दिन सक्नेछ र त्यस्तो निर्देशन पालना गर्नु प्रमाणीकरण निकायको कर्तव्य हुनेछ।

(६) उपदफा (५) बमोजिमको निर्देशनको पालना गरेमा वा उपदफा (१) बमोजिम शङ्का गरिएको आरोप पुष्टि नभएमा उपदफा (२) बमोजिम गरिएको इजाजतपत्रको निलम्बन फुकुवा हुनेछ।

(७) उपदफा (१) बमोजिमको जाँचबुझमा सहयोग पुऱ्याउनु प्रमाणीकरण निकायको कर्तव्य हुनेछ।

(८) उपदफा (१) बमोजिम गरिने जाँचबुझको सम्बन्धमा अपनाउनु पर्ने कार्यविधि तोकिए बमोजिम हुनेछ।

२२. **इजाजतपत्र रद्द गर्न सक्नेः** (१) नियन्त्रकले यस ऐन बमोजिम जारी गरेको इजाजतपत्र देहायको अवस्थामा जुनसुकै बखत रद्द गर्न सक्नेछ :-

(क) प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्न वा नवीकरणको लागि निवेदन दिँदाको बखत झुट्टा वा गलत विवरण तथा कागजात दाखिला गरेको देखिएमा,

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

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

(घ) यस ऐन बमोजिम नियन्त्रकले दिएको आदेश वा निर्देशनको उल्लङ्घन गरेमा।

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

२३. **निर्णयको जानकारी दिनुपर्नेः** दफा २१ बमोजिम इजाजतपत्र निलम्बन वा दफा २२ बमोजिम इजाजतपत्र रद्द गर्ने गरी गरेको निर्णयको जानकारी नियन्त्रकले त्यस्तो प्रमाणीकरण निकायलाई लिखित रुपमा दिनु पर्नेछ र त्यस्तो सूचना कम्प्युटर प्रणालीमा राखी राष्ट्रिय दैनिक पत्रिकामा तथा विद्युतीय स्वरुपमा समेत प्रकाशन गर्नु पर्नेछ।

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

(२) उपदफा (१) बमोजिमको निवेदन पर्न आएमा प्रमाणीकरण निकायले आवश्यक छानबिन गरी निवेदन प्राप्त भएको एक महिना भित्र सो सम्बन्धमा निर्णय गरिसक्नु पर्नेछ।

(३) उपदफा (२) बमोजिम प्रमाणीकरण निकायले प्रमाणपत्र जारी गर्ने निर्णय गरेमा पन्ध्र दिनभित्र आफ्नो हस्ताक्षर सहित प्रमाणपत्र जारी गर्नु पर्नेछ।

(४) उपदफा (३) बमोजिम प्रमाणपत्र जारी नगर्ने निर्णय गरेमा सोको कारण सहितको सूचना पन्ध्र दिनभित्र निवेदकलाई दिनु पर्नेछ।

२५. **प्रमाणपत्र जारी गर्न सक्ने**: यस ऐन बमोजिम इजाजतपत्र प्राप्त गरेको प्रमाणीकरण निकाय र दफा १६ को उपदफा (३) बमोजिम मन्त्रालयले तोकेको सरकारी निकायले मात्र डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र जारी गर्न सक्नेछ।

२६. **प्रमाणपत्र निलम्बन गर्न सक्ने**: प्रमाणीकरण निकायले देहायका अवस्थामा प्रमाणपत्र प्राप्त व्यक्तिको प्रमाणपत्र निलम्बन गर्न सक्नेछः-

(क) सार्वजनिक हित विपरीत हुने भई प्रमाणपत्र निलम्बन गर्नु पर्ने भएमा,

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

२७. **प्रमाणपत्र रद्द गर्न सक्ने**: (१) प्रमाणीकरण निकायले देहायका कुनै अवस्थामा प्रयोगकर्ताको प्रमाणपत्र रद्द गर्न सक्नेछः-

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

(ख) प्रमाणपत्र कायम राख्दा सार्वजनिक हित विपरीत हुने अवस्था भएमा,

(ग) प्रयोगकर्ताको मृत्यु भएमा,

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

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

(च) प्रमाणपत्रमा स्पष्ट पारिएको आधारभूत तथ्य झुट्ठा प्रमाणित भएमा, वा

(छ) प्रमाणपत्रको विश्वासनीयतामा तात्त्विक रुपमा असर पर्ने गरी जोडी साँचो सिर्जना गर्न प्रयोग गरिएको साँचो वा सुरक्षण प्रणालीमा फेरबदल वा काँटछाँट गरिएमा।

(२) उपदफा (१) बमोजिम प्रमाणपत्र रद्द गर्नु अघि सम्बन्धित प्रयोगकर्तालाई सफाइ पेश गर्ने मनासिब मौका दिनु पर्नेछ।

२८. **प्रमाणपत्र निलम्बन वा रद्द गरिएको सूचना**ः (१) दफा २६ बमोजिम प्रमाणपत्र निलम्बन वा दफा २७ बमोजिम प्रमाणपत्र रद्द गरिएकोमा त्यसरी प्रमाणपत्र निलम्बन गर्ने वा रद्द गर्ने प्रमाणीकरण निकायले सोको अभिलेख राखी त्यस्तो सूचना सार्वजनिक रुपमा प्रकाशन गर्नु पर्नेछ।

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

२९. **कार्यसम्पादन परीक्षण**ः (१) नियन्त्रकले प्रत्येक वर्ष प्रमाणीकरण निकायको कार्यसम्पादनको परीक्षण गर्नु, गराउनु पर्नेछ।

(२) उपदफा (१) बमोजिमको कार्यसम्पादन परीक्षण गर्नको लागि नियन्त्रकले सूचना तथा सञ्चार प्रविधि विषयमा कम्तीमा स्नातकोत्तर तह उत्तीर्ण गरेको र कम्प्युटर सुरक्षणको क्षेत्रमा कम्तीमा पाँच वर्षको अनुभव प्राप्त व्यक्तिलाई नियुक्त गर्न सक्नेछ।

(३) उपदफा (२) बमोजिम कार्यसम्पादन परीक्षण गर्नको लागि नियुक्त व्यक्तिले सम्झौता भएको मितिले तीन महिनाभित्र कार्य सम्पन्न गरी नियन्त्रक समक्ष कार्यसम्पादन परीक्षणको प्रतिवेदन पेश गर्नु पर्नेछ।

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

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

३०. **कम्प्युटर र तथ्याङ्कमा पहुँच पाउने**ः (१) कसैले डिजिटल हस्ताक्षर सम्बन्धमा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको उल्लङ्घन गरेको छ भन्ने शङ्का गर्नु पर्ने मनासिव कारण भएमा 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 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।

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

(२) उपदफा (१) बमोजिमको अभिलेख सुरक्षित राख्ने प्रयोजनको लागि डिजिटल हस्ताक्षरको गोपनीयता र सुरक्षालाई सुनिश्चित गर्न नियन्त्रकले देहाय बमोजिमको कार्य गर्नु पर्नेछः-

(क) कम्प्युटर सुरक्षण प्रणाली उपयोग गर्ने,

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

(ग) तोकिए बमोजिमको मापदण्डको पालना गर्ने।

(३) नियन्त्रकले सार्वजनिक साँचोको विवरण एउटै कम्प्युटर प्रणालीमा आबद्ध हुने गरी कम्प्युटर तथ्याङ्क प्रणालीमा अद्यावधिक 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।

३२. **विद्युतीय स्वरुपमा राख्न अनिवार्य नहुने** : (१) यस ऐनमा अन्यत्र जुनसुकै कुरा लेखिएको भए तापनि देहायका विषयहरू विद्युतीय स्वरुपमा राख्न अनिवार्य हुने छैनः-

(क) विनिमेय अधिकारपत्र ऐन, २०३४ मा उल्लेख भए बमोजिमका विनिमेय अधिकारपत्रहरु,

(ख) बकसपत्र, राजीनामा, बन्धकी, कबुलियतपत्र, ऋणपत्र वा त्यस्तै प्रकृतिका अचल सम्पत्तिको हक हस्तान्तरण गर्ने लिखतहरु,

(ग) अचल सम्पत्ति उपर हक वा स्वामित्व जनाउने अन्य कुनै लिखतहरु,

(घ) वारेसनामा, फिरादपत्र, प्रतिउत्तरपत्र वा अदालती काम कारबाहीमा प्रयोग हुने त्यस्तै प्रकृतिका अन्य लिखतहरु,

(ङ) दावीपत्र, प्रतिदावीपत्र, प्रतिवादपत्र वा मध्यस्थताको कारबाहीमा लिखितरुपमा पेश गर्नुपर्ने त्यस्तै प्रकृतिका अन्य लिखतहरु।

(२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी उपदफा (१) मा उल्लिखित विषयमा आवश्यकतानुसार थपघट गर्न सक्नेछ।

३३. **विवरण वा कागजात दाखिला गर्नु पर्नेः** यो ऐन वा यस ऐन अन्तर्गत बनेको नियम बमोजिम नियन्त्रक वा प्रमाणीकरण निकाय समक्ष कुनै विवरण, कागजात र प्रतिवेदन दाखिला गर्नु पर्ने जिम्मेवारी भएको व्यक्तिले तोकिएको म्यादभित्र त्यस्तो विवरण, कागजात र प्रतिवेदन दाखिला गर्नु पर्नेछ।

३४. **अधिकार प्रत्यायोजन गर्न सक्नेः** नियन्त्रकले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम बमोजिम आफूलाई प्राप्त अधिकार मध्ये न्यायिक अधिकार बाहेकका अन्य अधिकार आफ्नो मातहतका कुनै अधिकृत कर्मचारीले प्रयोग गर्ने गरी प्रत्यायोजन गर्न सक्नेछ।

परिच्छेद-४

प्रयोगकर्ताको काम, कर्तव्य र अधिकार

३५. **जोडी साँचो सिर्जना गर्नेः** (१) प्रमाणीकरण निकायबाट जारी गरिएको र ग्राहकद्वारा स्वीकार गरिएको प्रमाणपत्रमा सूचीकृत गरिनु पर्ने सार्वजनिक साँचो समावेश भएको जोडी साँचो ग्राहकले नै सिर्जना गर्नु पर्ने भएमा ग्राहकले त्यस्तो जोडी साँचो सिर्जना गर्दा सुरक्षित एसिमेट्रिक क्रिप्टो सिस्टमको प्रयोग गर्नु पर्नेछ ।

(२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि जोडी साँचो सिर्जना गर्न प्रयोग गर्नु पर्ने सुरक्षण प्रणालीको सम्बन्धमा प्रयोगकर्ता र प्रमाणीकरण निकायका बिचमा 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।

३६. **प्रमाणपत्र स्वीकार गरेको मानिने** : (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 प्रयोगकर्ताले प्रमाणपत्रलाई स्वीकार गरेको भएमा सो कारणबाट प्रयोगकर्ताले प्रमाणपत्रमा उल्लेख भएको कुनै सूचना माथि भर पर्ने व्यक्तिलाई देहायका कुराको 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 तथ्य सत्य भएको, र

(ग) प्रमाणपत्रमा उल्लेख भएका सूचना सत्य र दुरुस्त भएको।

३७. **निजी साँचोलाई सुरक्षित राख्नु पर्ने**: (१) प्रत्येक प्रयोगकर्ताले आफूले प्राप्त गरेको प्रमाणपत्रमा सूचीकृत गरिएको सार्वजनिक साँचोसँग सम्बन्धित निजी साँचोलाई सुरक्षित राख्नु पर्नेछ। डिजिटल हस्ताक्षर सिर्जना गर्ने अख्तियारी नपाएको कुनै पनि व्यक्तिलाई त्यस्तो साँचो बारे जानकारी नहुने गरी आवश्यक सबै उपाय अवलम्बन गर्नु पर्नेछ।

(२) प्रयोगकर्ताको निजी साँचोको सम्बन्धमा कसैलाई 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 यथाशीघ्र प्रमाणपत्र निलम्बन गर्नु पर्नेछ।

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

३८. **निजी साँचो नियन्त्रक समक्ष दाखिला गर्नु पर्ने**: (१) नेपालको सार्वभौमिकता वा अखण्डताको रक्षा गर्न वा मित्रराष्ट्रसँगको 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) बमोजिम दाखिला भएको निजी साँचो बारे नियन्त्रकले अनधिकृत व्यक्तिलाई जानकारी गराउन हुँदैन।

परिच्छेद-५

<u>डोमेन नाम, दर्ता तथा व्यवस्थापन</u>

३९. **<u>डोमेन नाम, व्यवस्थापन तथा नियमनः</u>** (१) डोमेन नाम, सोको व्यवस्थापन तथा नियमन विभागले गर्नेछ।

(२) डोमेन नाम सञ्चालनलाई भरपर्दो र सुरक्षित बनाउनको लागि विभागले डोमेन नाम सञ्चालकलाई आवश्यक निर्देशन दिन सक्नेछ।

४०. **<u>डोमेन नाम दर्ता गर्नु पर्नेः</u>** (१) कुनै व्यक्ति वा संस्थाले एनपी डोमेनमा नाम दर्ता गराउँदा विभागले तोकेको संस्थामा 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 वा मिल्दोजुल्दो हुने गरी डोमेन नाम दर्ता गर्न वा गराउन हुँदैन।

(४) सरकारी निकायले आफ्नो कार्यालयको डोमेन नाम गभर्मेन्ट डट एनपी (gov.np) अन्तर्गत दर्ता गर्नु पर्नेछ।

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

तर सरकारी निकायको डोमेन नाम नवीकरण गर्नु पर्ने छैन।

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

४१. **<u>डोमेन नाम सुरक्षित रहने</u>**: (१) देहाय बमोजिमका नाम दोस्रो र तेस्रो तहका डोमेन नामको लागि सुरक्षित रहनेछन्ः-

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

(ख) भौगोलिक वा पर्यटकीय स्थलको नाम,

(ग) पुरातात्त्विक वा धार्मिक महत्त्वको नाम,

(घ) राष्ट्रियरुपमा ख्याति प्राप्त व्यक्तिका नाम,

(ङ) सरकारी संस्थाको नाम,

(च) अन्तर्राष्ट्रिय गैरसरकारी संस्थाको नाम,

(छ) नेपाल सरकारले तोकेका अन्य नाम।

(२) उपदफा (१) को खण्ड (क), (घ) र (ङ) बमोजिमका डोमेन नाम सम्बन्धित संस्थाले मात्र र अन्य नाम मन्त्रालयले तोकेको निकायको स्वीकृति लिई जो कसैले प्रयोग गर्न पाउनेछ।

(३) उपदफा (१) बमोजिमका सुरक्षित नामसँग मिल्दोजुल्दो हुने गरी वा उक्त नामको महत्वलाई अवमूल्यन गर्ने गरी डोमेन नाम दर्ता गर्न वा गराउन हुँदैन।

४२. **<u>अनधिकृत रुपमा डोमेन नाम प्रणाली सञ्चालन गर्न नहुने</u>**: (१) कसैले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम विपरीत अनधिकृत रुपले डोमेन नाम प्रणाली सञ्चालन गर्न वा गराउन हुँदैन।

(२) उपदफा (१) बमोजिमको कार्य गरेमा विभागले एक लाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।

परिच्छेद-६

डाटा सेन्टर तथा क्लाउड सेवा सञ्चालन

४३. **<u>डाटा सेन्टर तथा क्लाउड सेवा सञ्चालन गर्न इजाजतपत्र लिनु पर्ने</u>:** (१) नेपालभित्र डाटा सेन्टर, क्लाउड वा दुवै सेवा सञ्चालन गर्न चाहने संस्थाले विभागबाट इजाजतपत्र लिनु पर्नेछ।

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

(२) उपदफा (१) बमोजिम इजाजतपत्र लिन विभागमा निवेदन दिनु पर्नेछ।

(३) उपदफा (२) बमोजिम निवेदन प्राप्त भएपछि जाँचवुझ गर्दा डाटा सेन्टर, क्लाउड वा दुवै सेवा सञ्चालन गर्न मापदण्ड पूरा गरेको पाइएमा विभागले इजाजपत्र दिनेछ।

(४) यो ऐन प्रारम्भ हुँदाका बखत सञ्चालनमा रहेका डाटा सेन्टर, क्लाउड वा दुवै सेवा प्रदायकले यो ऐन प्रारम्भ भएको एक वर्षभित्र यस दफा बमोजिमको इजाजतपत्र लिनु पर्नेछ।

(५) उपदफा (३) र (४) बमोजिम इजाजतपत्र प्राप्त संस्थाले वार्षिक रुपमा अद्यावधिक विवरण विभागमा पेश गर्नु पर्नेछ र विभागले वर्षको कम्तीमा दुई पटक अनुगमन गर्नु पर्नेछ।

(६) उपदफा (३) र (४) बमोजिमको इजाजतपत्र प्राप्त व्यक्तिले इजाजतपत्रको नवीकरण गर्न चाहेमा प्रत्येक दुई वर्षमा नवीकरण गर्नु पर्नेछ।

४४. **डाटा सेन्टर वा क्लाउडमा सूचना प्रणाली राख्न सक्नेः** (१) सरकारी निकायले तोकिए बाहेकका सूचना प्रणाली दफा ४३ बमोजिम इजाजतपत्र प्राप्त डाटा सेन्टर वा क्लाउडमा राखी सञ्चालन गर्न सक्नेछ।

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

४५. **इजाजतपत्र नलिई डाटा सेन्टर, क्लाउड वा दुवै सञ्चालन गर्न नहुने**ः (१) कसैले यस ऐन बमोजिम इजाजतपत्र नलिई डाटा सेन्टर, क्लाउड वा दुवै सञ्चालन गर्न हुँदैन।

(२) उपदफा (१) बमोजिम इजाजतपत्र नलिई डाटा सेन्टर, क्लाउड वा दुवै सञ्चालन गरेमा विभागले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।

परिच्छेद-७

साइबर सुरक्षा केन्द्र

४६. **केन्द्रको स्थापना :** (१) साइबर सुरक्षाको चुनौतिको अनुगमन र प्रतिकार्य समेतको लागि राष्ट्रिय साइबर सुरक्षा केन्द्र रहनेछ।

(२) केन्द्रको कार्यालय काठमाडौं उपत्यकामा रहनेछ ।

(३) केन्द्रको प्रमुखको रुपमा कार्य गर्न मन्त्रालयले सहसचिवस्तरको कर्मचारीलाई तोक्न सक्नेछ ।

(४) केन्द्रको काम सुचारु रुपले सञ्चालन गर्न आवश्यक सङ्ख्यामा कर्मचारी रहनेछन्।

४७. **केन्द्रको काम, कर्तव्य र अधिकारः** यस ऐनमा अन्यत्र उल्लिखित काम, कर्तव्य र अधिकारको अतिरिक्त केन्द्रको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) साइबर सुरक्षा जोखिमको अनुगमन तथा विश्लेषण गर्ने,

(ख) संवेदनशील सूचना पूर्वाधारको चौविसै घण्टा अनुगमन गर्ने तथा साइबर घटना तथा जोखिम मूल्याङ्कन गर्ने,

(ग) राष्ट्रिय सुरक्षा, प्रतिरक्षा, अर्थतन्त्र, जनस्वास्थ्य, सार्वजनिक शान्ति र व्यवस्था वा सार्वजनिक सुरक्षा वा अत्यावश्यक सेवामा पार्न सक्ने साइबर सुरक्षाका घटनाको प्रतिकार्य गर्ने,

(घ) संवेदनशील सूचना पूर्वाधारको पहिचान गरी निर्देशक समिति समक्ष पेश गर्ने,

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

(च) साइबर सुरक्षा सम्बन्धी प्राविधिक मापदण्ड तयार गरी निर्देशक समिति समक्ष पेश गर्ने,

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

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

(झ) साइबर सुरक्षाको घटनाका सम्बन्धमा अन्य मुलुकका कम्प्युटर आपतकालीन प्रतिकार्य समूहसँग समन्वय र सहकार्य गर्ने,

(ञ) साइबर सुरक्षा सम्बन्धी प्रविधिको अध्ययन, अनुसन्धान तथा विकासलाई प्रोत्साहन गर्ने तथा आवश्यकता अनुसार त्यस्ता कार्य गर्न विश्वविद्यालय वा सम्बन्धित सङ्घ संस्थासँग समन्वय र सहकार्य गर्ने,

(ट) साइबर चुनौतीको पहिचान, रोकथाम, प्रतिक्रिया तथा पुनर्लाभ लगायतका कामको साइबर सुरक्षा सेवा प्रदायकको रुपमा सूचीकरण गर्ने,

(ठ) कम्प्युटर वा कम्प्युटर प्रणालीको साइबर सुरक्षा निरीक्षण गर्ने,

(ड) आकस्मिक रुपमा आइपर्ने साइबर जोखिमलाई समाधान गर्नको लागि प्राविधिक जनशक्ति सहितको आकस्मिक सहायता समूहको गठन गर्ने,

(ढ) मानवीय वा प्राकृतिक कारणले हानी नोक्सानी पुगी राष्ट्रिय सुरक्षा, अर्थ व्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य वा सार्वजनिक सुरक्षासँग सम्बन्धित सूचना प्रविधि प्रणाली बन्द भएमा यथाशीघ्र सो प्रणालीलाई पुनः सञ्चालनमा ल्याउन सहयोग गर्ने,

(ण) सूचना प्रविधि र साइबर सुरक्षा सम्बन्धी घटनाको अध्ययन तथा विश्लेषण गरी सम्बन्धित निकाय वा व्यक्तिलाई जानकारी गराउने तथा सोको समाधानको लागि सहजीकरण गर्ने,

(त) आवश्यकता अनुसार विषयगत तथा क्षेत्रगत सहायता समूह गठन गर्ने र सो समूहको काम कारबाहीको अनुगमन गर्ने, गराउने,

(थ) विषयगत तथा क्षेत्रगत सहायता समूहको गठन, कार्यक्षेत्र र सञ्चालन सम्बन्धी कार्यविधि बनाई निर्देशक समिति समक्ष पेश गर्ने, र

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

४८. **केन्द्रले निर्देशन दिन सक्ने:** (१) केन्द्रले यो ऐन बमोजिम कार्य गर्न संवेदनशील सूचना पूर्वाधारका धनी, अनुमतिपत्र प्राप्त सेवा प्रदायक तथा साइबर सुरक्षा परीक्षकलाई निर्देशन दिन सक्नेछ र त्यस्तो निर्देशनको पालना गर्नु सम्बन्धित संवेदनशील सूचना पूर्वाधारका धनी, अनुमतिपत्र प्राप्त सेवा प्रदायक तथा साइबर सुरक्षा परीक्षकको कर्तव्य हुनेछ।

(२) उपदफा (१) बमोजिमको निर्देशन पालना नगरेमा केन्द्रले एक लाख रुपैयाँसम्म जरिबाना गर्नेछ।

४९. **वार्षिक प्रतिवेदन:** (१) केन्द्रले प्रत्येक आर्थिक वर्ष समाप्त भएको मितिले तीन महिना भित्र आफूले सम्पादन गरेको काम कारबाहीको प्रतिवेदन तयार गरी मन्त्रालय समक्ष पेश गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिमको प्रतिवेदनमा अन्य कुराका अतिरिक्त केन्द्रले प्राप्त गरेको बजेट तथा कार्यक्रम र सो कार्यक्रम सञ्चालन गर्दा हुन गएको खर्च, मुख्य मुख्य कामको विवरण तथा उपलब्धि र भविष्यमा गर्नु पर्ने सुधार समेतका विषय समावेश गर्नु पर्नेछ।

परिच्छेद-८

साइबर सुरक्षा सेवा प्रदायकको सूचीकरण

५०. **साइबर सुरक्षा सेवा प्रदान गर्न सूचीकृत हुनु पर्ने:** (१) साइबर सुरक्षा सेवा प्रदान गर्न चाहने व्यक्ति, कम्पनी वा संस्था साइबर सुरक्षा सेवा प्रदायकको रुपमा केन्द्रमा सूचीकृत हुनु पर्नेछ।

(२) सार्वजनिक संस्थाले साइबर सुरक्षा सेवा लिँदा उपदफा (१) बमोजिम सूचीकृत साइबर सुरक्षा सेवा प्रदायकबाट लिनु पर्नेछ।

५१. **सूचीकृत हुन निवेदन दिने:** (१) दफा ५० बमोजिम सूचीकृत हुन 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 मुल्य अभिवृद्धि कर वा स्थायी लेखा नम्बर दर्ताको प्रमाणपत्र,

(घ) कम्पनी अद्यावधिक भएको पत्र,

(ङ) अघिल्लो आर्थिक वर्षको कर चुक्ता प्रमाणपत्र,

(च) कम्पनी वा संस्थाको सञ्चालक समितिको विवरण,

(छ) व्यक्तिको हकमा नेपाली नागरिकताको प्रमाणपत्र वा राष्ट्रिय परिचयपत्रको प्रतिलिपि।

५२. **सूचीकृत गर्ने:** (१) दफा ५१ 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 साइबर सुरक्षा सेवा प्रदायकको रुपमा सूचीकृत गर्नेछ।

(२) सूचीकरणको मान्य अवधि सूचीकृत भएको मितिले तीन वर्षको हुनेछ।

(३) यस ऐन बमोजिम सूचीकृत व्यक्ति, कम्पनी वा संस्थाले साइबर सुरक्षा सम्बन्धी सेवा प्रदान गरेको विवरणको वार्षिक रुपमा तोकिए बमोजिमको ढाँचामा अभिलेख राख्नु पर्नेछ ।

५३. **अद्यावधिक र अभिलेख:** (१) सूचीकृत व्यक्तिले सूची अद्यावधिक गर्न चाहेमा दफा ५२ को उपदफा (२) बमोजिमको अवधि समाप्त हुनु भन्दा कम्तीमा तीस दिन अघि अद्यावधिक गर्नको लागि देहायका कागजात संलग्न गरी केन्द्रमा निवेदन दिनु पर्नेछः-

(क) सूचीकृत संस्थाले प्रदान गरेको साइबर सुरक्षा सेवाको वार्षिक विवरण,

(ख) कम्पनी वा संस्थाको हकमा कर चुक्ता प्रमाणपत्र र कम्पनी अद्यावधिक भएको पत्र।

(२) उपदफा (१) बमोजिम प्राप्त निवेदन उपर जाँचबुझ गर्दा निवेदकले सूचीकृत गर्दाको बखत तोकिएको सर्त पालना गरेको देखिएमा केन्द्रले दुई वर्षको लागि अद्यावधिक गर्न सक्नेछ।

(३) केन्द्रले सूचीकृत साइबर सुरक्षा सेवा प्रदायकको अभिलेख राख्नु पर्नेछ।

परिच्छेद-९

संवेदनशील सूचना पूर्वाधार र साइबर सुरक्षा परीक्षक

५४. **संवेदनशील सूचना पूर्वाधार तोक्ने:** केन्द्रको सिफारिसमा नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशित गरी संवेदनशील सूचना पूर्वाधार तोक्न सक्नेछ।

५५. **संवेदनशील सूचना पूर्वाधार सम्बन्धी जानकारी माग गर्न सक्ने:** (१) केन्द्रले संवेदनशील सूचना पूर्वाधारका धनीसँग देहायका विषयमा जानकारी माग गर्न सक्नेछः-

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

(ख) संवेदनशील सूचना पूर्वाधारसँग जोडिएका वा सूचना आदानप्रदान गर्ने कम्प्युटर वा कम्प्युटर प्रणालीको डिजाइन, कन्फिगुरेसन तथा सुरक्षा र सोसँग सम्बन्धित कम्प्युटर प्रणालीको सञ्चालन सम्बन्धी जानकारी।

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

तर प्रचलित नेपाल कानूनले त्यस्तो जानकारी दिन रोक लगाएको भएमा यस दफा बमोजिम जानकारी दिन बाध्य गरेको मानिने छैन।

५६. **साइबर सुरक्षा अनुगमन र परीक्षणः** (१) संवेदनशील सूचना पूर्वाधारको धनीले कम्तीमा वर्षको एक पटक दफा ५९ बमोजिमको परीक्षकबाट संवेदनशील सूचना पूर्वाधारको सुरक्षा परीक्षण गराई उक्त परीक्षण प्रतिवेदन केन्द्र समक्ष पेश गर्नु पर्नेछ।

(२) उपदफा (१) बमोजिम साइबर सुरक्षा परीक्षण सन्तोषजनक नदेखिएमा केन्द्रले पुनः परीक्षण गराउन निर्देशन दिन सक्नेछ। त्यस्तो परीक्षणको प्रतिवेदन संवेदनशील सूचना पूर्वाधार धनीले केन्द्र समक्ष पेश गर्नु पर्नेछ।

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

(४) केन्द्रले संवेदनशील सूचना पूर्वाधारको अनुगमन गर्ने व्यवस्था गर्नेछ।

५७. **साइबर सुरक्षाका घटनाको जानकारी गराउनु पर्नेः** संवेदनशील सूचना पूर्वाधारका धनीले साइबर सुरक्षाको घटना घटेमा त्यस्तो घटना लगत्तै देहायका विषयमा केन्द्रलाई जानकारी गराउनु पर्नेछः-

(क) संवेदनशील सूचना पूर्वाधार प्रणालीको धनीले आफूले सञ्चालन गरेको संवेदनशील पूर्वाधार प्रणालीसँग सञ्चार आदानप्रदान गर्ने गरी जोडिएको कुनै कम्प्युटर वा कम्प्युटर प्रणालीसँग सम्बन्धित साइबर सुरक्षा घटना,

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

५८. **साइबर सुरक्षा अभ्यास गराउनु पर्नेः** संवेदनशील सूचना पूर्वाधारका धनीले कुनै साइबर सुरक्षा घटनामा प्रतिक्रिया गर्न तत्पर अवस्थामा राखे नराखेको परीक्षण गर्न समय समयमा साइबर सुरक्षा अभ्यास गर्नु पर्नेछ।

५९. **साइबर सुरक्षा परीक्षक सूचीकृत हुनुपर्ने:** (१) साइबर सुरक्षा परीक्षण गर्न चाहने व्यक्ति वा संस्थाले साइबर सुरक्षा परीक्षकको रुपमा 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 प्रत्येक बर्ष सूची अद्यावधिक गर्नु पर्नेछ।

(४) साइबर सुरक्षा परीक्षकको रुपमा सूचीकृत हुन केन्द्रमा देहायका कागजात पेश गर्नु पर्नेछः-

(क) संस्था दर्ताको प्रमाणपत्र,

(ख) मूल्य अभिवृद्धि कर वा स्थायी लेखा नम्बर दर्ताको प्रमाणपत्र,

(ग) करचुक्ताको प्रमाणपत्र, र

(घ) सम्बन्धित व्यक्तिको हकमा नेपाली नागरिकताको प्रमाणपत्र वा राष्ट्रिय परिचयपत्र, शैक्षिक प्रमाणपत्र, तालिमको प्रमाणपत्र, व्यवसायिक प्रमाणपत्रको प्रतिलिपि।

(५) सूचीकरणका लागि आवश्यक योग्यता, मापदण्ड र साइबर सुरक्षा परीक्षकको कार्य तोकिए बमोजिमको हुनेछ।

(६) उपदफा (१) बमोजिम सूचीकृत नभइ कुनै व्यक्ति वा संस्थाले साइबर सुरक्षा परीक्षकको रुपमा काम गरेमा केन्द्रले पचास हजार रुपैयाँसम्म जरिबाना गर्न सक्नेछ।

६०. **सूचीकृत गर्नु पर्ने:** केन्द्रले तोकेको साइबर सुरक्षासँग सम्बन्धित हार्डवेयर उत्पादन र आपूर्ति सम्बन्धी कार्य गर्ने व्यक्ति, साइबर सुरक्षासँग सम्बन्धित भनी केन्द्रले तोकेको सफ्टवेयर विकास र आपूर्ति सम्बन्धी कार्य गर्ने व्यक्ति र सो हार्डवेयर तथा सफ्टवेयर सञ्चालनका सम्बन्धमा परामर्श तथा अन्य सेवा उपलब्ध गर्ने व्यक्ति तोकिए बमोजिम केन्द्रमा सूचीकृत हुनु पर्नेछ।

परिच्छेद-१०

बैयक्तिक विवरण तथा सूचनाको सुरक्षा

६१. **वैयक्तिक विवरणको सङ्कलनः** (१) कसैले वैयक्तिक विवरण सङ्कलन गर्नु परेमा सो विवरण कुन प्रयोजनको लागि आवश्यक परेको हो त्यस्तो प्रयोजन खुलाई सम्बन्धित व्यक्तिसँग अनुमति लिनु पर्नेछ।

(२) सूचना प्रविधि प्रणालीमा रहेका कुनै व्यक्तिको वैयक्तिक विवरण सङ्कलन गर्दा खुलाईएको प्रयोजन बाहेक अन्य प्रयोजनका लागि प्रयोग, प्रसार तथा आदानप्रदान गर्न पाईने छैन।

तर सम्बन्धित व्यक्तिको स्वीकृतिमा अन्य प्रयोजनका लागि प्रयोग तथा प्रसार गर्न बाधा परेको मानिने छैन।

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

६२. **सूचना सुरक्षाको सुनिश्चितता गर्नु पर्नेः** (१) प्रशोधनकर्ता, सञ्चयकर्ता र सेवा प्रदायकले विद्युतीय स्वरुपमा रहेका सूचनाको आदानप्रदान, प्रशोधन तथा सञ्चय गर्दा निर्धारित मापदण्डको आधारमा सुरक्षाको सुनिश्चितता गर्नु पर्नेछ।

(२) सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्य सम्बन्धी सेवा प्रदाय संस्थाले तोकिएको विवरण इन्क्रिप्ट गरी सुरक्षित राख्नु पर्नेछ।

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

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

६३. **सुरक्षा मापदण्ड अवलम्बन गर्नु पर्नेः** सरकारी निकाय तथा सार्वजनिक संस्थाले कम्प्युटर तथा सूचना प्रणालीको प्रयोग गर्दा सुरक्षा मापदण्ड अवलम्बन गर्नु पर्नेछ।

६४. **सेवा प्रदायकले दायित्व ब्यहोर्नु नपर्नेः** (१) प्रचलित कानूनमा जुनसुकै कुरा लेखिएको भए तापनि देहायको अवस्थामा सेवा प्रदायकले कुनै तेस्रो पक्षको सूचना वा तथ्याङ्क वा लिङ्कमा पहुँच उपलब्ध गराएको कारणबाट मात्र उक्त सूचना वा तथ्याङ्क वा लिङ्कमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणको सम्बन्धमा उत्पन्न हुने कुनै दायित्व व्यहोर्नु पर्ने छैनः-

(क) सूचना, तथ्याङ्क वा लिङ्कमा पहुँच पुर्‍याउने कार्यमा मात्र सीमित रहेको भएमा,

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

(ग) आफ्नो सूचना प्रणालीमा भण्डारण गरेको कुनै खास सूचना गैरकानूनी रहेको भनी कुनै सम्बन्धित सार्वजनिक निकाय वा अदालतबाट त्यस्तो

सूचना सामग्री हटाउन वा त्यस्ता सूचनामा पहुँच निष्क्रीय पार्न प्राप्त आदेश बमोजिम सेवा प्रदायकले सूचना सामग्री यथाशीघ्र हटाएमा वा पहुँच निष्क्रीय बनाएमा,

(घ) नियामक निकायको सम्बन्धित निर्देशन पालना गरेको भएमा।

(२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि कुनै सूचना, तथ्याङ्क वा लिङ्कमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणले प्रचलित कानूनको उल्लङ्घन गरेमा वा कुनै गैरकानूनी कार्य गर्न दुरुत्साहन वा सहयोग गरेमा सेवा प्रदायक त्यस्तो दायित्वबाट मुक्त हुने छैन।

६५. <u>सूचना सुरक्षित राख्नु पर्नेः</u> सेवा प्रदायकले सेवा प्रयोग सम्बन्धी तोकिए बमोजिमका सूचना तोकिएको अवधिसम्म सुरक्षित राख्नु पर्नेछ ।

परिच्छेद-११

<u>सूचना प्रविधि तथा साइबर सुरक्षा निर्देशक समिति</u>

६६. <u>निर्देशक समितिको गठन</u> : (१) सूचना प्रविधि तथा साइबर सुरक्षाको क्षेत्रमा नीतिगत मार्गदर्शन गर्न देहाय बमोजिमको सूचना प्रविधि तथा साइबर सुरक्षा निर्देशक समिति रहनेछः-

(क) सञ्चार तथा सूचना प्रविधि मन्त्री -अध्यक्ष

(ख) गभर्नर, नेपाल राष्ट्र बैङ्क -सदस्य

(ग) सचिव, प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय -सदस्य

((घ) सचिव, गृह मन्त्रालय -सदस्य

(ङ) सचिव, मन्त्रालय -सदस्य

(च) अध्यक्ष, नेपाल दूरसञ्चार प्राधिकरण -सदस्य

((छ) सूचना प्रविधि वा साइबर सुरक्षाको क्षेत्रमा स्नाकोत्तर उपाधि हासिल गरी कम्तीमा पन्ध्र वर्ष काम गरी ख्यातिप्राप्त गरेका व्यक्तिमध्येबाट मन्त्रालयले मनोनयन गरेको कम्तीमा एकजना महिला सहित दुई जना -सदस्य

(ज) महानिर्देशक, राष्ट्रिय साइबर सुरक्षा केन्द्र -सदस्य

(झ) सहसचिव (प्राविधिक), मन्त्रालय -सदस्य-सचिव

(२) उपदफा (१) को खण्ड (ञ) बमोजिमका मनोनित सदस्यको पदावधि दुई वर्षको हुनेछ।

(३) उपदफा (२) मा जुनसुकै कुरा लेखिएको भए तापनि मनोनित सदस्यको कार्यसम्पादन सन्तोषजनक नभएमा वा पद अनुकूलको आचरण पालना नगरेमा मन्त्रालयले त्यस्तो सदस्यलाई जुनसुकै बखत पदबाट हटाउन सक्नेछ।

तर त्यसरी पदबाट हटाउँदा निजलाई सफाइ पेश गर्ने मनासिब मौका दिनु पर्नेछ।

६७. **निर्देशक समितिको काम, कर्तव्य र अधिकारः** निर्देशक समितिको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी नीति तथा कानूनमा सुधार गर्नका लागि नेपाल सरकार समक्ष सिफारिस गर्ने,

(ख) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी प्राविधिक मापदण्ड स्वीकृतिको लागि नेपाल सरकार, मन्त्रिपरिषद् समक्ष पेश गर्ने,

(ग) सूचना प्रविधि प्रणाली र पूर्वाधारको एकरुपता तथा अन्तरआवद्धताको लागि सहजीकरण गर्ने,

(घ) विद्युतीय सुशासनको लागि सम्बन्धित निकायलाई उत्तरदायी बनाउने तथा शासन प्रणालीको तीनै तहसम्म विद्युतीय शासन विस्तार गर्न सहजीकरण गर्ने,

(ङ) सूचना प्रविधिको क्षेत्रमा रोजगारीका अवसर विस्तार गर्न सरकारी तथा निजी क्षेत्रको सहकार्य तथा साझेदारीलाई प्रवर्द्धन गर्न सहजीकरण गर्ने,

(च) कृत्रिम बौद्धिकता (ए.आई.) को अनुसन्धान, विकास तथा प्रयोगलाई प्रोत्साहन गर्ने,

(छ) सूचना प्रविधि, साइबर सुरक्षा तथा कृत्रिम बौद्धिकताको प्रयोगको सम्बन्धमा प्रदेश, स्थानीय तह तथा अन्य सम्बद्ध निकाय बिच आवश्यक समन्वय गर्ने,

(ज) केन्द्रको सिफारिसमा संवेदनशील सूचना पूर्वाधारको धनीले पालना गर्नु पर्ने सर्त, सुरक्षाको उपायका सम्बन्धमा निर्देशन दिने वा सो सम्बन्धी आवश्यक मापदण्ड स्वीकृत गर्ने, र

(झ) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी आवश्यक अन्य कार्य गर्ने।

६८. **निर्देशक समितिको बैठकः** (१) निर्देशक समितिको बैठक आवश्यकतानुसार बस्नेछ।

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

(३) निर्देशक समितिको बैठकको अध्यक्षता समितिको अध्यक्षले गर्नेछ।

(४) निर्देशक समितिको बैठकमा बहुमतको राय मान्य हुनेछ र मत बराबर भएमा बैठकमा अध्यक्षता गर्ने व्यक्तिले निर्णायक मत दिनेछ।

(५) निर्देशक समितिको बैठकको निर्णय बैठकमा उपस्थित सबै सदस्यबाट प्रमाणित गरी अभिलेख राख्नु पर्नेछ।

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

परिच्छेद–१२

विद्युतीय माध्यमबाट सेवा प्रवाह

६९. **विद्युतीय माध्यमबाट सार्वजनिक सेवा प्रदान गर्न सकिने** : (१) सरकारी निकाय तथा सार्वजनिक संस्थाले आफूले प्रदान गर्ने सार्वजनिक सेवा विद्युतीय माध्यमबाट उपलब्ध गराउन सक्नेछन्।

(२) उपदफा (१) को प्रयोजनको लागि नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकेका सार्वजनिक सेवा तोकिएको समयावधि भित्र विद्युतीय माध्यमबाट सम्बन्धित निकायले उपलब्ध गराउनु पर्नेछ।

(३) प्रदेश सरकार तथा स्थानीय तहले सार्वजनिक सेवा प्रवाह गर्दा सम्भव भएसम्म विद्युतीय माध्यमको प्रयोग गर्नु पर्नेछ।

(४) उपदफा (२) र (३) बमोजिमका सेवा प्रवाह गर्दा विद्युतीय पहिचान (ई-केवाइसी) को व्यवस्था गरी कार्यान्वयनमा ल्याउनु पर्नेछ।

७०. **सूचना विद्युतीय स्वरूपमा राख्नु पर्ने** : (१) सरकारी निकाय वा सार्वजनिक संस्थाले आफूले सिर्जना, सङ्कलन तथा प्राप्त गरेका सूचना विद्युतीय स्वरुपमा पनि राख्नु पर्नेछ।

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

(३) उपदफा (१) बमोजिमको सूचना पुनःप्रयोग गर्न मिल्ने गरी समयबद्ध रुपमा अभिलेखीकरण गर्नु पर्नेछ।

७१. **विद्युतीय माध्यमबाट कारोबार गर्न र अभिलेख राख्न सक्नेः** सरकारी निकाय वा सार्वजनिक संस्था वा नेपालभित्र कारोबार गर्ने बैङ्क वा वित्तीय संस्थाले प्रचलित कानून बमोजिम राख्नु

पर्ने अभिलेख तथा गरिने कारोबार विद्युतीय स्वरुप वा विद्युतीय सञ्चार माध्यमको प्रयोग गरी अभिलेख राख्न वा कारोबार गर्न सक्नेछ।

७२. **सूचना प्रविधि प्रणाली प्रयोग गर्नु पर्ने**: (१) सरकारी निकाय तथा सार्वजनिक संस्थाले तोकिएको मापदण्ड बमोजिमको सूचना प्रविधि प्रणालीको प्रयोग गर्नु पर्नेछ।

(२) सरकारी निकाय तथा सार्वजनिक संस्थाले सूचना प्रविधि प्रणाली मार्फत खुला मानक (ओपन स्टयाण्डर्ड) मा सूचना संरक्षण गरी राख्न सक्नेछन्।

(३) उपदफा (१) बमोजिम सरकारी निकायले सूचना प्रविधि प्रणालीको प्रयोग गर्दा एक अर्का बिच अन्तरआबद्धता हुने गरी तथ्याङ्क तथा सूचना आदानप्रदान गर्नु पर्नेछ।

(४) सरकारी निकायले सूचना प्रविधि प्रणाली सञ्चालन गर्नु पूर्व उपदफा (१) बमोजिमको मापदण्ड अनुरुप भए नभएको परीक्षण तोकिएको निकायबाट गराउनु पर्नेछ।

७३. **डिजिटल हस्ताक्षर प्रयोग गर्न सक्ने**: सरकारी निकाय र सार्वजनिक संस्थाले आफ्नो कार्य सम्पादन वा सेवा प्रवाह गर्दा यस ऐन बमोजिमको डिजिटल हस्ताक्षर प्रयोग गर्न सक्नेछन्।

७४. **वेबसाइट सञ्चालनमा ल्याउनु पर्ने** : (१) प्रत्येक सरकारी निकाय र सार्वजनिक संस्थाले सूचना तथा सेवा प्रवाह गर्न आफ्नो वेबसाइटको विकास र सञ्चालन गर्नु पर्नेछ।

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

७५. **सूचना प्रविधि प्रणालीको स्वामित्व हस्तान्तरण गर्ने**: (१) दफा ७२ बमोजिमको सूचना प्रविधि प्रणाली वा दफा ७४ बमोजिमको वेबसाइट निर्माणकर्ताले त्यस्तो सूचना प्रविधि प्रणाली वा वेबसाइटसँग सम्बन्धित सोर्स कोड, टेक्निकल डकुमेन्टेसन तथा क्रिडेन्सियल (युजर नेम र पासवर्ड) सहितको सम्पूर्ण संरचना त्यस्तो सूचना प्रविधि प्रणाली वा वेबसाइट सञ्चालन गर्ने सार्वजनिक निकायलाई हस्तान्तरण गर्नु पर्नेछ।

(२) यो ऐन प्रारम्भ हुँदाका बखत सञ्चालनमा रहेका सरकारी निकायको सूचना प्रविधि प्रणाली वा वेबसाइटको सोर्स कोड, टेक्निकल डकुमेन्टेसन तथा क्रिडेन्सियल (युजर नेम र पासवर्ड) सहितको सम्पूर्ण संरचनाहरु सार्वजनिक निकायसँग निर्माण तथा सञ्चालन सम्झौता गरिएको भए सो सम्झौतामा उल्लिखित अवधिभित्र र त्यस्तो सम्झौता नभएमा यो ऐन प्रारम्भ भएको मितिले तीन महिनाभित्र हस्तान्तरण गर्नु पर्नेछ।

(३) उपदफा (१) वा (२) बमोजिम सूचना प्रविधि प्रणाली वा वेबसाइटको सोर्स कोड, टेक्निकल डकुमेन्टेसन तथा क्रिडेन्सियल (युजर नेम र पासवर्ड) सहितको सम्पूर्ण संरचनाहरु हस्तान्तरण नगर्ने निर्माणकर्तालाई विभागले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।

७६. **<u>सूचना प्रविधि सम्बन्धी प्राविधिक परीक्षण:</u>** (१) नेपाल सरकारले सरकारी निकायमा प्रयोगमा रहेका सूचना प्रविधि प्रणाली, पूर्वाधार तथा कार्यप्रणालीको आन्तरिक प्राविधिक परीक्षण गर्नका लागि मन्त्रालय अन्तर्गतको कुनै निकायलाई तोक्न सक्नेछ ।

(२) उपदफा (१) बमोजिमको तोकिएको निकायले देहाय बमोजिम हुने गरी परीक्षण गर्ने गराउनेछः-

(क) नेपाल सरकारका संवेदनशील सूचना प्रविधि प्रणाली र पूर्वाधारको कम्तीमा वर्षमा एक पटक प्राविधिक परीक्षण गर्ने गराउने,

(ख) सरकारी निकायको अनुरोधको आधारमा सूचना प्रविधि प्रणाली र पूर्वाधारको प्राविधिक परीक्षण गर्ने गराउने,

(३) उपदफा (२) बमोजिम परीक्षण सम्पन्न भएपछि परीक्षण गर्ने निकायले सूचना प्रविधि प्रणाली र पूर्वाधारको पूर्णता, दोहोरोपना, सुरक्षा स्थितिको सम्बन्धमा सुझाव सहितको प्रतिवेदन सम्बन्धित निकायलाई उपलब्ध गराउनु पर्नेछ।

परिच्छेद-१३

<u>सूचना प्रविधि उद्योग तथा उपकरण</u>

७७. **<u>जानकारी दिनु पर्ने:</u>** सूचना प्रविधि सम्बन्धी उद्योग स्थापना भएपछि सोको जानकारी विभागलाई दिनु पर्नेछ।

७८. **<u>स्वीकृत मापदण्डका उपकरण मात्र पैठारी तथा बिक्री वितरण गर्नु पर्ने:</u>** (१) सूचना प्रविधि सम्बन्धी तोकिए बमोजिमका उपकरणको हकमा स्वीकृत मापदण्डको आधारमा मात्र पैठारी तथा बिक्री वितरण गर्न पाइनेछ।

(२) उपदफा (१) बमोजिमको मापदण्ड, उपकरणको गुणस्तर, आयु र सुरक्षाको आधारमा स्वीकृत गर्ने प्रक्रिया सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।

७९. **<u>नवीनतम प्रविधिको प्रयोग:</u>** (१) सूचना प्रविधिको क्षेत्रमा विकसित भएका नवीनतम प्रविधिको पारदर्शी, जवाफदेही, सुरक्षित र मर्यादित प्रयोग गर्नु पर्नेछ।

<u>स्पष्टीकरण:</u> यस दफाको प्रयोजनको लागि "नवीनतम प्रविधि" भन्नाले सूचना प्रविधिको क्षेत्रमा नयाँ र द्रुत गतिमा विकसित भएका कृत्रिम बौद्धिकता, मेसिन लर्निङ्ग, ब्लकचेन, ईन्टरनेट अफ थिङ्गस, फाइभ जी तथा नेक्सट जेनरेसन नेटवर्क, क्वान्टम कम्प्युटिङ्ग लगायतका प्रविधि सम्झनु पर्छ।

(२) उपदफा (१) बमोजिमको नवीनतम् प्रविधिको उपयोग, प्रवर्धन र विस्तार सरकारी, सार्वजनिक र निजी क्षेत्रको सहकार्यमा गर्न सकिनेछ।

(३) उपदफा (१) बमोजिमको नवीनतम प्रविधिको व्यवस्थित प्रयोगको लागि विभागले समन्वय र सहजीकरण गर्नेछ।

परिच्छेद-१४

कसूर र सजाय

८०. **मुलुकको साइबर सुरक्षा तथा तथ्याङ्क प्रणालीमा अवरोध सिर्जना गर्न नहुने:** (१) कसैले विद्युतीय प्रणालीको प्रयोग गरी मुलुकको साइबर सुरक्षा तथा तथ्याङ्क प्रणालीमा अवरोध सिर्जना गर्ने वा प्रतिकूल असर पार्ने कुनै कार्य गर्न वा गराउन हुदैन।

(२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी पाँच वर्षसम्म कैद वा दशलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

८१. **विद्युतीय प्रणालीको कार्य सञ्चालनमा हस्तक्षेप गर्न नहुने:** (१) कसैले आफू वा अरु कसैलाई आर्थिक वा अन्य लाभ पुऱ्याउने नियतले अनधिकृत रुपमा विद्युतीय सूचना प्रविष्ट वा सम्प्रेषण वा हेरफेर गरी वा मेटाई वा लुकाई छिपाई विद्युतीय प्रणालीको कार्य सञ्चालनमा हस्तक्षेप गर्न वा कसैलाई आर्थिक नोक्सानी हुने गरी निजको संवेदनशील वित्तीय सूचना प्राप्त गर्न वा गराउन हुँदैन।

(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी तीन वर्षसम्म कैद वा पाँचलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

८२. **विद्युतीय प्रणालीको स्रोत सङ्केत नष्ट, परिवर्तन गर्न वा चोरी गर्न नहुने:** (१) कसैले विद्युतीय प्रणालीमा प्रयोग हुने स्रोत सङ्केत तथा सूचनाको चोरी गर्न, अनधिकृत रुपमा नष्ट गर्न वा परिवर्तन गर्न हुँदैन।

स्पष्टीकरण: यस दफाको प्रयोजनका लागि "स्रोत सङ्केत" भन्नाले कम्प्युटर कार्यक्रमको सूचीकरण, कम्प्युटर निर्देशन, कम्प्युटर डिजाइन र कम्प्युटर लेआउट तथा कम्प्युटर सम्पदाको जुनसुकै स्वरुपमा रहेको कार्यक्रम विश्लेषण सम्झनु पर्छ।

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

(३) उपदफा (१) वा (२) बमोजिमको कसूर गरेमा कसूरको मात्र हेरी तीन वर्षसम्म कैद वा पाँचलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

८३. **कम्प्युटर प्रणालीमा अनधिकृत पहुँच पुऱ्याउन, सूचना प्रविष्ट गर्न, हेरफेर गर्न नहुने**ः (१) कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीमा अनधिकृत

पहुँच पुऱ्याउन वा त्यस्तो प्रणालीमा प्रवेश गरी डाटाको अखण्डतामा फरक पर्ने गरी डाटा हेरफेर गर्ने वा मेटाउने कार्य गर्नु वा गराउनु हुँदैन।

(२) 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 हुँदैन।

(३) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुई लाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

८४. **<u>विद्युतीय प्रणालीमा अवरोध गर्न नहुने</u>** : (१) कसैले कुनै विद्युतीय प्रणालीको कार्य सञ्चालनमा बाधा पुऱ्याउन वा प्रयोगकर्तालाई प्रणाली प्रयोगमा अबरोध गर्न, रोक लगाउन वा हस्तक्षेप गर्न हुँदैन।

(२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी तीन वर्षसम्म कैद वा तीनलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

८५. **<u>विद्युतीय स्वरुपको सूचनालाई क्षति पुऱ्याउन, अवरोध गर्न नहुने</u>**: (१) कसैले गलत मनसाय राखी कसैको स्वामित्व वा नियन्त्रणमा रहेको विद्युतीय स्वरुपको सूचनालाई अनधिकृत रुपमा मेटाउन, नष्ट गर्न, हेरफेर गर्न, बिगार्न, बुझ्न नसकिने गरी परिवर्तन गर्न वा अर्थहीन, प्रयोगहीन वा निष्प्रभावी गराउन वा सूचनाको प्रयोगलाई अनधिकृत रुपमा बाधा पुऱ्याउन, रोक लगाउन वा आधिकारिक व्यक्तिलाई सूचनामा पहुँच दिन ईन्कार गर्न हुँदैन।

(२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्र हेरी तीन वर्षसम्म कैद वा तीनलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

८६. **<u>गोपनीयता भङ्ग गर्न नहुने</u>**: (१) कसैले यस ऐन विपरीत विद्युतीय माध्यमबाट कसैको वैयक्तिक विवरण संकलन गरेमा वा सूचना, जानकारी अनधिकृत रूपमा प्राप्त गर्न, त्यसको गोपनीयता भङ्ग गर्न वा अनधिकृत रूपमा कसैलाई उपलब्ध गराउन हुँदैन।

(२) कसैले पनि कुनै दुई वा दुईभन्दा बढी व्यक्तिबिचमा विद्युतीय माध्यमबाट भएका कुनै वैयक्तिक संवाद वा कुराकानी वा सङ्केत सम्बन्धित व्यक्तिले 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,

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

(ख) प्रचलित कानून बमोजिमको अवस्थामा कुनै पनि सूचना वा जानकारीको ध्वनि अङ्कन वा रेकर्ड गर्न वा गराउन सकिनेछ।

(३) उपदफा (१) वा (२) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा तीनलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

८७. **झुट्टा प्रमाणपत्र प्रकाशन गर्न वा उपलब्ध गर्न, गराउन नहुने:** (१) कसैले प्रमाणीकरण निकायले प्रमाणपत्र जारी गरेको होइन वा सो प्रमाणपत्रमा सूचीकृत गरिएको ग्राहकले स्वीकार गरेको छैन वा सो प्रमाणपत्र निलम्बन वा रद्द भइसकेको छ भन्ने जानीजानी त्यस्तो प्रमाणपत्रको प्रकाशन गर्न वा अन्य कसैलाई कुनै ब्यहोराले उपलब्ध 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 गराइएको विषयमा यस दफा बमोजिम कसूर मानिने छैन।

(२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रूपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

८८. **अश्लील सामग्री उत्पादन, वितरण, प्रकाशन, प्रसार वा खरिद बिक्री गर्न वा गराउन नहुने:** (१) कसैले विद्युतीय प्रणालीको माध्यमबाट कुनै अश्लिल सामग्रीको उत्पादन तथा सङ्कलन गर्न, बिक्री वितरण गर्न, प्रकाशन गर्न, प्रदर्शन गर्न, प्रसार गर्न वा सञ्चय गर्न हुँदैन।

तर कुनै व्यक्तिले कुनै अनुसन्धान, कानून कार्यान्वयन, अध्यापन वा चिकित्सकीय प्रयोजनको लागि यौनजन्य सामग्रीको सम्प्रेषण, प्राप्ति वा सञ्चय गरेको प्रमाणिक रूपमा देखाउन सकेमा र त्यस्तो उद्देश्य पूरा हुनासाथ त्यस्ता सामग्री मेटाएमा यस दफा बमोजिमको कसूर मानिने छैन।

(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

८९. **गोप्य कोड चोरी गर्न नहुने:** (१) 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।

स्पष्टीकरण: यस दफाको प्रयोजनको लागि,-

(क) "फिसिङ्ग" भन्नाले विद्युतीय सञ्चार माध्यमबाट कुनै कुरा सत्य हो भन्ने विश्वासमा पारी कुनै व्यक्तिको युजरनेम र पासवर्ड, क्रेडिट कार्ड नम्बर, बैङ्क एकाउन्ट जस्ता संवेदनशील सूचना प्राप्त गर्ने कार्य सम्झनु पर्छ र सो शब्दले नक्कली लिङ्क प्रयोग गरी साइबर स्पेसका प्रयोगकर्तालाई झुक्याई

संवेदनशील जानकारी प्रवाह गर्न प्रेरित गर्ने वा कुनै मालवेयर स्थापना गर्ने कार्य सम्झनु पर्छ।

(ख) "स्पुफिङ" भन्नाले कसैले अज्ञात स्रोतबाट भएको सञ्चारलाई ज्ञात र विश्वसनीय स्रोतबाट आएको भनी झुक्याउने कार्य सम्झनु पर्छ।

(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

९०. **कम्प्युटर प्रणालीबाट डाटा चोरी गर्न नहुनेः** (१) कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीबाट वा स्निफिङ लगायतका विधि प्रयोग गरी नेटवर्कमा प्रसारित डाटालाई चोरी गर्नु वा गराउनु हुँदैन।

स्पष्टीकरणः यस दफाको प्रयोजनको लागि "स्निफिङ" भन्नाले कसैले दुई वा सोभन्दा बढी पक्ष बिच भएको डाटा आदानप्रदानमा सम्बन्धित पक्षको अनुमति बिना अनधिकृत रुपमा उक्त डाटा सुन्ने, पढ्ने वा हेर्ने कार्य सम्झनु पर्छ।

(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

९१. **कम्प्युटर प्रणालीमा अवाञ्छित एप्लिकेशन फैलाउन नहुनेः** (१) कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको कम्प्युटर वा कम्प्युटर प्रणालीमा अनुमतिबिना अवाञ्छित एप्लिकेशन प्रवेश गराउने वा फैलाउने कार्य गर्नु वा गराउनु हुँदैन।

(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

९२. **सार्वजनिक सूचना प्रणालीमा अवरोध गर्न नहुनेः** (१) कसैले सार्वजनिक प्रयोगमा रहेको कम्प्युटर वा कम्प्युटर प्रणालीको सञ्जाललाई डिनायल अफ सर्भिस लगायतका विधि प्रयोग गरी बन्द गर्ने वा कम्प्युटर प्रणालीको अपेक्षित प्रयोगकर्ताका लागि कम्प्युटर प्रणालीमा पहुँच नपुग्ने वातावरण सिर्जना हुने कार्य गर्नु वा गराउनु हुँदैन।

स्पष्टीकरणः यस दफाको प्रयोजनको लागि "डिनायल अफ सर्भिस" भन्नाले कसैले सार्वजनिक रुपमा सेवा प्रदान गर्ने कम्प्युटर प्रणाली बन्द गर्ने वा उक्त प्रणालीबाट प्रदान गरिने सेवा अवरुद्ध हुने गरी आक्रमण गर्ने कार्य सम्झनु पर्छ।

(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

९३. **इन्टरनेट अफ थिङ्गसमा आक्रमण गर्न नहुनेः** (१) कसैले इन्टरनेट अफ थिङ्गसमा आधारित उपकरण तथा सञ्जालमा अनुमति बिना आक्रमण गरी सो सञ्जालको निर्धारित काममा खलल पुऱ्याउने कार्य गर्नु वा गराउनु हुँदैन।

स्पष्टीकरणः यस दफाको प्रयोजनको लागि "इन्टरनेट अफ थिङ्गस" भन्नाले एक अर्का बिच डाटा आदानप्रदान गर्न सक्ने इलेक्ट्रोमेकानिकल उपकरणको सामूहिक सञ्जाल सम्झनु पर्छ।

(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

९४. **पहिचानको दुरुपयोग गर्न नहुनेः** (१) कसैले विद्युतीय माध्यममा रहेको व्यक्तिको निजी साँचो, पासवर्ड वा अन्य विद्युतीय स्वरुपमा रहेको पहिचानको स्थानान्तरण, नियन्त्रण वा प्रयोग गरी प्रचलित कानून बमोजिम कसूर मानिने कार्य गर्ने मनसायले पहिचानको दुरुपयोग गर्नु हुँदैन।

(२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी एक वर्षसम्म कैद वा एकलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

९५. **कृत्रिम बौद्धिकता (आर्टिफिसियल इन्टेलिजेन्स) को प्रयोग गरी कसूर गरेमा सजाय हुनेः** कसैले यस ऐन बमोजिम कसूर मानिने कार्य कृत्रिम बौद्धिकता (आर्टिफिसियल इन्टेलिजेन्स) को प्रयोग गरी गरेमा त्यस्तो कसूर सोही व्यक्तिले गरे सरह मानी सजाय हुनेछ।

९६. **कसूर गर्न दुरुत्साहन गर्न नहुनेः** कसैले यस ऐन बमोजिमको कुनै कसूर गर्न दुरुत्साहन गरेमा वा अपराधिक षडयन्त्रमा संलग्न भएमा त्यस्तो व्यक्तिलाई मुख्य कसूरदारलाई भए सरहको सजाय हुनेछ।

९७. **मतियारलाई हुने सजायः** यस ऐन बमोजिमको कुनै कसूर गर्न सघाउने वा अन्य कुनै ब्यहोराले मतियार भई कार्य गर्ने व्यक्तिलाई मुख्य कसूरदारलाई भएको सजायको आधा सजाय हुनेछ।

९८. **सङ्गठित संस्थाबाट भएको कसूरः** कुनै फर्म वा कम्पनी वा सङ्गठित संस्थाले यस ऐन बमोजिमको कसूर मानिने कुनै काम गरे वा गराएमा त्यस्तो कार्य गर्ने गराउने व्यक्ति जिम्मेवार हुनेछ र त्यस्तो व्यक्ति किटान हुन नसकेमा फर्म, कम्पनी वा सङ्गठित संस्थाको हकमा कार्यकारी प्रमुख भई काम गर्ने सम्बन्धित धनी वा हिस्सेदार, सञ्चालक, प्रबन्ध सञ्चालक वा महाप्रबन्धकले आपराधिक दायित्व ब्यहोर्नु पर्नेछ।

९९. **प्रचलित कानून बमोजिम सजाय गर्न बाधा नपर्नेः** 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।

१००. **<u>क्षतिपूर्ति भराउनु पर्नेः</u>** यस ऐन बमोजिम कसूर गरेको कारणबाट कसैलाई कुनै किसिमको हानी, नोक्सानी, हैरानी वा क्षति भएको रहेछ भने त्यस्तो हानी, नोक्सानी, हैरानी वा क्षतिको क्षतिपूर्ति सम्बन्धित कसूरदारबाट भराई दिनु पर्नेछ।

१०१. **<u>नेपाल सरकार वादी हुनेः</u>** (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।

१०२. **<u>हदम्यादः</u>** यो ऐन बमोजिमको कसूर भए गरेको थाहा पाएको मितिले छ महिना भित्र उजुर गर्नु पर्नेछ।

१०३. **<u>पुनरावेदनः</u>** (१) ऐनको दफा १६ को उपदफा (५) र दफा २० को उपदफा (६) बमोजिम नियन्त्रकले गरेको जरिवाना, दफा ४२ को उपदफा (२), दफा ४५ को उपदफा (२) र दफा ७५ को उपदफा (३) बमोजिम विभागले गरेको जरिवाना र दफा ४८ को उपदफा (२) र दफा ५९ को उपदफा (६) बमोजिम केन्द्रले गरेको जरिवाना उपर चित्त नबुझेमा त्यस्तो निर्णय भएको थाहा पाएको मितिले पैंतिस दिनभित्र जिल्ला अदालतमा पुनरावेदन गर्न सकिनेछ।

परिच्छेद-१५

<u>अनुसन्धान तथा प्रमाण</u>

१०४. **<u>अनुसन्धान अधिकृतः</u>** (१) यस ऐन बमोजिमको कसूर सम्बन्धी मुद्दाको अनुसन्धान सूचना प्रविधि सम्बन्धी ज्ञान भएको कम्तीमा प्रहरी निरीक्षकस्तरको अधिकृतले गर्नेछ।

(२) उपदफा (१) बमोजिम अनुसन्धान गर्दा अनुसन्धान अधिकृतले प्राविधिक विषयमा विभागसँग समन्वय गर्न सक्नेछ।

१०५. **<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 पहुँचबाट हटाईन सक्ने सम्भावना रहेको कुरामा अनुसन्धान अधिकृत विश्वस्त भएमा त्यस्तो विद्युतीय उपकरण वा सूचना नियन्त्रणमा रहेको व्यक्तिलाई अनुसन्धान अधिकृतले लिखित सूचना दिई बढीमा सात दिनसम्म 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 अनुसन्धान अधिकृतको आदेशको पालना गर्नु सम्बन्धित व्यक्तिको कर्तव्य हुनेछ।

१०६. **<u>ट्राफिक तथ्याङ्कमा पहुँच पुऱ्याउन सक्नेः</u>** कुनै खास सञ्चारसँग सम्बद्ध ट्राफिक तथ्याङ्क कुनै कसूरको अनुसन्धान प्रयोजनको लागि अदालतले तत्काल प्राप्त प्रमाणको आधारमा आवश्यक ठानेमा अनुसन्धान अधिकृतलाई खास सञ्चार सम्बन्धी ट्राफिक तथ्याङ्कमा पहुँच राख्न अनुमति दिन सक्नेछ।

१०७. **<u>ट्राफिक तथ्याङ्कको सङ्कलनः</u>** (१) कुनै खास सञ्चारसँग सम्बन्धित ट्राफिक तथ्याङ्क कुनै कसूरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक देखेमा उक्त ट्राफिक तथ्याङ्कमा नियन्त्रण गर्न देहाय बमोजिमको आदेश गर्न सक्नेछः-

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

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

(२) कुनै खास सञ्चारसँग 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 सङ्कलन वा अभिलेखन गर्न अनुमति प्रदान गर्न सक्नेछ।

१०८. **<u>विषयवस्तुको अन्तरदोहन (इन्टरसेप्सन):</u>** (१) सञ्चारको कुनै विषयवस्तु कसूरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक देखेमा सेवा प्रदायकलाई प्रविधिको प्रयोग गरी विद्युतीय प्रणाली मार्फत प्रसार भएको खास सञ्चारको विषयवस्तु प्रसार हुँदाहुँदैको अवस्थामा सङ्कलन 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 देखेमा सञ्चारको विषयवस्तु प्रसार हुँदाहुँदैको अवस्थामा सङ्कलन वा अभिलेख गर्न अनुसन्धान अधिकृतलाई अख्तियारी प्रदान गर्न सक्नेछ।

१०९. **<u>विद्युतीय प्रमाणको ग्राह्यताः</u>** कुनै कसूर विरुद्धको कारबाहीको क्रममा प्रचलित कानून बमोजिम विद्युतीय प्रणालीबाट सिर्जना भएको विद्युतीय वा अन्य कुनै स्वरुपमा रहेको कुनै सूचना वा तथ्याङ्क प्रमाणको रुपमा ग्राह्य हुनेछ।

परिच्छेद-१६

विविध

१११०. **अनुसन्धान तथा तालिम केन्द्र स्थापना र सञ्चालनः** नेपाल सरकारले सूचना प्रविधि तथा साइबर सुरक्षाको सम्बन्धमा अध्ययन, अनुसन्धान तथा विकास गर्न र सो सम्बन्धी विषयमा तालिम सञ्चालन गर्न अनुसन्धान तथा तालिम केन्द्रको स्थापना र सञ्चालन गर्न सक्नेछ।

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

(२) उपदफा (१) ले दिएको अधिकारको सर्वसामान्यतामा प्रतिकूल प्रभाव नपर्ने गरी देहायको विषयमा नियम बनाउन सकिनेछः-

(क) सुरक्षित विद्युतीय अभिलेख तथा परीक्षण विधि,

(ख) विद्युतीय अभिलेखको प्राप्ति,स्वीकार तथा सोको जानकारी,

(ग) डिजिटल हस्ताक्षर, डिजिटल हस्ताक्षरको सुरक्षण कार्यविधि तथा परीक्षण र सम्पुष्टि,

(घ) नियन्त्रक तथा प्रमाणीकरण निकायको काम, कर्तव्य र अधिकार,

(ङ) प्रमाणीकरण निकायको योग्यता, इजाजतपत्र र सोको दस्तुर, इजाजतपत्रको निलम्बन तथा रद्द गर्ने तथा नवीकरण र सेवा शुल्क,

(च) विदेशी प्रमाणीकरण निकायलाई मान्यता दिँदा अपनाउनु पर्ने कार्यविधि,

(छ) डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र, प्रमाणपत्रको निलम्बन, फुकुवा वा रद्द,

(ज) कार्यसम्पादन परीक्षकको योग्यता, नियुक्ति, सेवा अवधि, पारिश्रमिक र परीक्षण,

(झ) विद्युतीय माध्यमबाट प्रदान गरिने सरकारी सेवा, सेवा प्राप्त गर्ने प्रक्रिया,

(ञ) प्रयोगकर्ताले जोडी साँचो सिर्जना गर्दा अपनाउनु पर्ने प्रक्रिया,

(ट) विद्युतीय माध्यमबाट गरिने कारोबारको अभिलेख तथा भुक्तानी,

(ठ) डोमेन नाम दर्ता, नवीकरण तथा दस्तुर, एनपी डोमेन नाम सञ्चालन,

(ड) सूचना प्रविधि सम्बन्धी उद्योग र व्यवसाय सञ्चालनको स्वीकृति, नवीकरण र खारेज,

(ढ) सूचना प्रविधि सम्बन्धी उपकरणको पैठारी तथा बिक्री वितरण,

(ण) नवीनतम प्रविधिको प्रयोग,

(त) सरकारी तथा सार्वजनिक निकायमा प्रयोग भएको सूचना प्रविधिको सुरक्षाको परीक्षण,

(थ) डाटा सेन्टर वा क्लाउडको इजाजतपत्र, सोको नवीकरण शुल्क तथा दस्तुर,

(द) साइबर सुरक्षा प्रदायक सूचीकृत सम्बन्धी,

(प) संवेदनशील सूचना पूर्वाधार, र

(प) अनुसन्धान तथा तालिम केन्द्रको स्थापना र सञ्चालन।

११२. <u>**मापदण्ड बनाउनेः**</u> यो ऐन कार्यान्वयन गर्न मन्त्रालयले देहायको विषयमा मापदण्ड बनाउन सक्नेछः-

(क) विद्युतीय सूचना तथा डिजिटल हस्ताक्षरको गोपनीयता र सुरक्षा,

(ख) सरकारी निकायमा कम्प्युटर तथा सूचना प्रविधि प्रणालीको प्रयोग,

(ग) सरकारी निकाय तथा सार्वजनिक संस्थाको वेबसाइट,

(घ) सूचना प्रविधि प्रणाली र पूर्वाधारको प्राविधिक परीक्षण,

(ङ) डाटा सेन्टर वा क्लाउड सेवा मापदण्ड, र

(च) साइबर सुरक्षाको मापदण्ड।

११३. <u>**खारेजी र बचाउः**</u> (१) विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ खारेज गरिएको छ।

(२) विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ बमोजिम भए गरेका काम कारबाही यसै ऐन बमोजिम भए गरेको मानिनेछ।

सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा व्यवस्था गर्न बनेको विधेयक

क्र.स.	दफा	दफा शिर्षक	व्याख्यात्मक टिप्पणी
१.	२	परिभाषा	यस दफामा ऐनमा पटक पटक प्रयोग भएका शब्दहरूलाई परिभाषित गरिएको छ।
२.	३	विद्युतीय अभिलेखले कानूनी मान्यता पाउने	यस दफामा यो ऐन वा यस ऐन अन्तर्गत बनेको नियममा उल्लिखित प्रक्रिया पूरा गरी प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेखको लिखित, मुद्रित वा अन्य कुनै स्वरुपमा हुनु पर्ने भनी उल्लेख गरिएको विषय विद्युतीय स्वरुपमा अभिलेख राख्न सकिनेछ र त्यस्तो विद्युतीय अभिलेखले कानूनी मान्यता प्राप्त गर्ने व्यवस्था गरिएको छ।
३.	४	सुरक्षित राख्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेख कुनै खास अवधिसम्म सुरक्षित राख्नु पर्ने भनी उल्लेख गरिएकोमा त्यस्तो सूचना, लिखत, तथ्याङ्क वा अभिलेख विद्युतीय स्वरुपमा पनि सोही अवधिसम्म सुरक्षित राख्नु पर्नेछ । (२) उपदफा (१) बमोजिमको सुरक्षित राखिएको विद्युतीय अभिलेखले देहायका सर्त पूरा गरेमा 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, र (ग) उत्पत्ति, गन्तव्य र सम्प्रेषण वा प्राप्तिको मिति तथा समय पहिचान गर्न सकिने विवरण उपलब्ध हुने गरी राखिएको भएमा।
४.	५	मूल वा सक्कल अभिलेखको रुपमा पेश गर्न सकिने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रचलित कानूनमा मूल वा सक्कल अभिलेख नै पेश गर्नु पर्ने वा सुरक्षित राख्नु पर्ने भनी उल्लेख गरिएकोमा देहाय बमोजिमका सर्त पूरा भएमा त्यस्तो मूल वा सक्कल अभिलेखको विद्युतीय प्रति पेश गर्न सकिनेछः- (क) विद्युतीय स्वरुपमा सिर्जना गरिएको समयदेखि सो अभिलेखमा कुनै पनि किसिमबाट परिवर्तन गरिएको छैन भनी विश्वास गर्न सकिने 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।
५.	६	सुरक्षित विद्युतीय अभिलेख मानिने	यस दफामा सुरक्षण कार्यविधि अपनाई सिर्जना गरिएको विद्युतीय अभिलेख तोकिए बमोजिम परीक्षण गर्दा कुनै किसिमको हेरफेर गरिएको छैन भन्ने यकिन भएमा त्यस्तो विद्युतीय अभिलेखलाई सुरक्षित विद्युतीय अभिलेख मानिने व्यवस्था गरिएको छ।
६.	७	उत्पत्तिकर्ताको अभिलेख मानिने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) देहायका अवस्थामा कुनै विद्युतीय अभिलेख उत्पत्तिकर्ताको अभिलेख मानिनेछः- (क) उत्पत्तिकर्ता आफैंले त्यस्तो विद्युतीय अभिलेख सम्प्रेषण गरेको भएमा, (ख) विद्युतीय अभिलेखको सम्बन्धमा आवश्यक कार्य गर्न उत्पत्तिकर्ताको तर्फबाट अख्तियारी प्राप्त गरेको व्यक्तिले त्यस्तो विद्युतीय अभिलेख सम्प्रेषण गरेको भएमा, र (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 आधारमा तत्सम्बन्धी कार्य गर्ने अधिकार प्राप्त गर्नेछ।
७.	८	विद्युतीय अभिलेखको प्राप्ति र स्वीकार गर्ने प्रक्रिया	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) उत्पत्तिकर्ताले विद्युतीय अभिलेख पठाउँदाका बखत वा पठाउनुभन्दा अगावै प्रापकलाई सो विद्युतीय अभिलेख प्राप्त भएको सूचना वा जानकारी पठाउन अनुरोध गरेको वा त्यसरी सूचना वा जानकारी पठाउन उत्पत्तिकर्ता र प्रापकको बिचमा सहमति भएको अवस्थामा त्यस्तो विद्युतीय अभिलेखको प्राप्ति स्वीकार गर्ने सम्बन्धमा उपदफा (२), (३) र (४) का व्यवस्था लागू हुनेछन्।

			(२) विद्युतीय अभिलेख प्राप्त भएको सूचना वा जानकारी कुनै खास ढाँचामा वा कुनै खास तरिकाबाट दिनु पर्ने गरी उत्पत्तिकर्ता र प्रापकबिचमा कुनै सम्झौता नभएको अवस्थामा त्यस्तो सूचना वा जानकारी 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) उत्पत्तिकर्ता र प्रापकको बीचमा कुनै विद्युतीय अभिलेखको सम्बन्धमा त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्रापकबाट प्राप्त गरेपछि मात्र निजको हकमा बन्धनकारी हुने भनी सहमति भएकोमा त्यस्तो सूचना वा भरपाई प्राप्त नभएसम्म प्रापकको हकमा बन्धनकारी 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 उत्पत्तिकर्ता वा प्रापकबिच कुनै समय निर्धारण वा मञ्जुरी नभएको भए तोकिए बमोजिमको समयभित्र उत्पत्तिकर्ताले प्रापकबाट त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्राप्त गरिसकेको मानिनेछ।
८.	९	सम्प्रेषण र प्राप्तिको समय तथा स्थान	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) उत्पत्तिकर्ता र प्रापकबिचमा अन्यथा सम्झौता भएकोमा बाहेक कुनै विद्युतीय अभिलेख उत्पत्तिकर्ताको नियन्त्रण बाहिरको सूचना प्रविधि प्रणालीमा प्रवेश गरेपछि त्यस्तो विद्युतीय अभिलेखको सम्प्रेषण भएको मानिनेछ। (२) उत्पत्तिकर्ता र प्रापकबिचमा अन्यथा सम्झौता भएकोमा बाहेक कुनै विद्युतीय अभिलेखको प्राप्तिको समय र स्थान तोकिए बमोजिम निर्धारण गरिनेछ। (३) उत्पत्तिकर्ता र प्रापकबिचमा अन्यथा सम्झौता भएकोमा बाहेक कुनै विद्युतीय अभिलेखलाई उत्पत्तिकर्ताको व्यवसाय सञ्चालन हुने स्थानबाट सम्प्रेषण गरेको र प्रापकको व्यवसाय सञ्चालन हुने स्थानमा प्राप्त भएको मानिनेछ।

			स्पष्टीकरण: यस उपदफाको प्रयोजनको लागि "व्यवसाय सञ्चालन हुने स्थान" भन्नाले,- (क) उत्पत्तिकर्ता वा प्रापकको एकभन्दा बढी व्यवसाय सञ्चालन हुने स्थान रहेको अवस्थामा सम्बन्धित कारोबारसँग सम्बद्ध रहेको व्यवसाय सञ्चालन हुने स्थान सम्झनु पर्छ। (ख) उत्पत्तिकर्ता वा प्रापकको कुनै व्यवसाय सञ्चालन हुने स्थान नभएको अवस्थामा निजको बसोबासको स्थानलाई नै निजको व्यवसाय सञ्चालन हुने स्थान सम्झनु पर्छ।
९.	१०	डिजिटल हस्ताक्षर	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेखलाई हस्ताक्षरबाट प्रमाणित गर्नु पर्ने भएमा त्यस्तो काम डिजिटल हस्ताक्षरबाट गर्न सकिनेछ। (२) उपदफा (१) को प्रयोजनको लागि डिजिटल हस्ताक्षरको सिर्जना गर्न देहायको सर्त 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, र (ग) डिजिटल हस्ताक्षर गरिसकेपछि सम्बन्धित अभिलेख तथा हस्ताक्षर परिवर्तन भए नभएको पत्ता लगाउन सकिने भएमा।
१०.	११	डिजिटल हस्ताक्षरको कानूनी मान्यता	यस दफामा प्रचलित कानूनमा कुनै सूचना, लिखत, तथ्याङ्क वा अभिलेखलाई हस्ताक्षरद्वारा प्रमाणित गर्नु पर्ने वा कुनै लिखतमा कुनै व्यक्तिको हस्ताक्षर गरिएको हुनु पर्ने भनी उल्लेख गरिएको रहेछ भने त्यस्ता सूचना, लिखत, तथ्याङ्क 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 गर्ने व्यवस्था गरिएको छ।
११.	१२	सुरक्षित डिजिटल हस्ताक्षर मानिने	यस दफामा यस ऐन बमोजिम सुरक्षण कार्यविधि अपनाई परीक्षण र सम्पुष्टि गरिएको कुनै विद्युतीय अभिलेखमा रहेको डिजिटल हस्ताक्षरलाई सुरक्षित डिजिटल हस्ताक्षर मानिने व्यवस्था गरिएको छ।

१२.	१३	डिजिटल हस्ताक्षरको शुल्क निर्धारण	यस दफामा प्रमाणीकरण निकायले डिजिटल हस्ताक्षर सम्बन्धी सेवा उपलब्ध गराए बापत प्रयोगकर्तासँग लिने शुल्क सम्बन्धी व्यवस्था तोकिए बमोजिम हुने व्यवस्था गरिएको छ।
१३.	१४	नियन्त्रक तोक्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) इजाजतपत्र जारी गर्ने, सो सम्बन्धमा आवश्यक समन्वय तथा नियमन गर्ने प्रयोजनको लागि एक नियन्त्रकको कार्यालय रहनेछ। (२) नियन्त्रकको कार्यालयको प्रमुखको रुपमा काम गर्न नेपाल सरकारले निजामती सेवाको कुनै सेवा/समूहको राजपत्राङ्कित प्रथम श्रेणीको अधिकृतलाई नियन्त्रक तोक्नेछ। (३) यो ऐन प्रारम्भ हुँदाको बखत कायम रहेको नियन्त्रकको कार्यालय यसै ऐन बमोजिम स्थापना भएको नियन्त्रक कार्यालय मानिनेछ।
१४.	१५	नियन्त्रकको काम, कर्तव्य र अधिकार	यस दफामा यस ऐनमा अन्यत्र उल्लिखित काम, कर्तव्य र अधिकारको अतिरिक्त नियन्त्रकको प्रमाणीकरण निकाय सम्बन्धी काम, कर्तव्य र अधिकार देहाय बमोजिम हुने व्यवस्था गरिएको छः- (क) इजाजतपत्र प्रदान गर्ने, (ख) इजाजतपत्र निलम्बन गर्ने वा रद्द गर्ने, (ग) काम कारबाहीको सुपरिवेक्षण तथा रेखदेख गर्ने र आवश्यकता अनुसार निर्देशन दिने, (घ) डिजिटल हस्ताक्षरको सम्पुष्टि गर्ने सम्बन्धमा कायम गर्नु पर्ने स्तर निर्धारण गर्ने, (ङ) आफ्नो कारोबार सञ्चालन गर्दा पालन गर्नु पर्ने सर्त निर्धारण गर्ने, (च) प्रमाणपत्रको ढाँचा र त्यसभित्र समाविष्ट हुनु पर्ने विषय वस्तुको निर्धारण गर्ने, (छ) यस परिच्छेद बमोजिम प्रकट गरेका सूचनाको अभिलेख खडा गरी सार्वजनिक रुपमा पहुँचयोग्य हुने गरी तथ्याङ्कको व्यवस्था गर्ने र सो तथ्याङ्कलाई अद्यावधिक गर्ने, (ज) वार्षिक कार्यसम्पादन परीक्षण गर्ने, गराउने, र (झ) डिजिटल हस्ताक्षरको प्रमाणपत्र सम्बन्धी कार्य गर्ने ।सम्पर्क विन्दुको ठेगाना परिवर्तन हुँदा वा गुनासो सुन्ने अधिकारी परिवर्तन हुँदा सोको सूचना विभागलाई दिई सोको सूचना सर्वसाधारणको जानकारीको लागि

			समेत सार्वजनिक रुपमा प्रकाशन गर्नु पर्ने व्यवस्था गरिएको छ।
१५.	१६	प्रमाणीकरण निकायले इजाजतपत्र लिनुपर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्ने, निलम्बन वा रद्द गर्ने काम समेतको लागि प्रमाणीकरण निकायले यस ऐन बमोजिम इजाजतपत्र लिनु पर्नेछ। (२) उपदफा (१) बमोजिमको इजाजतपत्र प्राप्त नगरी कसैले पनि प्रमाणीकरण निकायको रुपमा कार्य गर्न वा गराउन हुँदैन। (३) उपदफा (१) र (२) मा जुनसुकै कुरा लेखिएको भए तापनि नियन्त्रकको कार्यालयमा सूचीकृत हुने गरी मन्त्रालयले कुनै सरकारी निकायलाई प्रमाणीकरण निकायको रुपमा काम गर्न तोक्न सक्नेछ। (४) उपदफा (३) बमोजिम तोकिएको निकायले सरकारी निकायको लागि डिजिटल हस्ताक्षरको प्रमाणपत्र जारी गर्न, निलम्बन वा रद्द गर्न सक्नेछ। (५) उपदफा (२) बमोजिम इजाजतपत्र प्राप्त नगरी प्रमाणीकरण निकायको रुपमा कार्य गर्ने वा गराउनेलाई नियन्त्रकले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।
१६.	१७	प्रमाणीकरण गर्ने विदेशी निकायलाई मान्यता दिन सक्नेः	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) नियन्त्रकले कुनै विदेशी मुलुकको कानून बमोजिम प्रमाणपत्र जारी गर्ने इजाजतपत्र प्राप्त गरेको प्रमाणीकरण गर्ने निकायलाई नेपाल सरकारको पूर्व स्वीकृति लिई नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकिए बमोजिमको शर्त पालना गर्ने गरी मान्यता दिन सक्नेछ। यसरी मान्यता प्राप्त गरेको प्रमाणीकरण गर्ने विदेशी निकायले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम अन्तर्गत प्रमाणपत्र जारी गर्न सक्नेछ । (२) उपदफा (१) बमोजिम मान्यता प्राप्त प्रमाणीकरण गर्ने निकायको नेपालमा शाखा कार्यालय रहेको हुनु पर्नेछ।
१७.	१८	इजाजतपत्रको लागि निवेदन दिनु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) दफा १६ बमोजिम प्रमाणीकरण निकायको रुपमा काम गर्न तोकिए बमोजिमको योग्यता पुगेका व्यक्तिले तोकिए बमोजिमको दस्तुर सहित इजाजतपत्र प्राप्त गर्न देहाय बमोजिमका कागजात संलग्न गरी नियन्त्रक समक्ष निवेदन दिनु पर्नेछ :- (क) प्रमाणीकरण सम्बन्धी विवरण, (ख) निवेदकको पहिचान तथा सनाखतको पुष्टि हुने कागजात,

			(ग) जनशक्ति, वित्तीय तथा भौतिक स्रोत खुल्ने कागजात। (२) दफा १६ को उपदफा (३) बमोजिमको सरकारी निकायलाई उपदफा (१) को खण्ड (ग) बमोजिमको कागजात र इजाजतपत्र दस्तुर आवश्यक पर्ने छैन।
१८.	१९	इजाजतपत्र दिनु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) दफा १८ बमोजिम इजाजतपत्रको लागि प्राप्त निवेदन उपर जाँचबुझ गर्दा उपयुक्त देखिएमा नियन्त्रकले तोकिएको ढाँचामा इजाजतपत्र दिनु पर्नेछ। (२) उपदफा (१) बमोजिमको इजाजतपत्रको विवरण सार्वजनिक रुपमा प्रकाशित गर्नु पर्नेछ।
१९.	२०	इजाजतपत्र नवीकरण गर्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रमाणीकरण निकायले प्राप्त गरेको इजाजतपत्र प्रत्येक दुई वर्षमा नवीकरण गर्नु पर्नेछ। (२) उपदफा (१) बमोजिम इजाजतपत्रको नवीकरण गर्न चाहने प्रमाणीकरण निकायले 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 आवश्यक जाँचबुझ गरी इजाजतपत्रको अवधि समाप्त हुनुभन्दा एक महिना अघि निर्णय गरिसक्नु पर्नेछ। (४) उपदफा (३) बमोजिम नवीकरण सम्बन्धी जाँचबुझ तथा निर्णय गर्दा दफा २९ बमोजिमको कार्यसम्पादन परीक्षण प्रतिवेदन समेतलाई आधारको रुपमा लिन सकिनेछ। (५) नियन्त्रकले इजाजतपत्र नवीकरण नगर्ने निर्णय गर्नु अघि निवेदकलाई आफ्नो सफाई पेश गर्ने मनासिब मौका दिनु पर्नेछ। (६) उपदफा (१) बमोजिम नवीकरण नगरी प्रमाणीकरण निकायको रुपमा काम गर्ने व्यक्ति वा संस्थालाई नियन्त्रकले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।
२०.	२१	जाँचबुझ तथा इजाजतपत्र निलम्बन गर्न	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्नको लागि नियन्त्रक समक्ष पेश गरेको कागजात, विवरण र वित्तीय तथा भौतिक स्रोत झुट्ठा भएमा वा

		सक्ने	कारोबार सञ्चालन गर्दा पालन गर्नु पर्ने सर्तको पालना नगरेमा वा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको उल्लङ्घन गरेको शंका गर्नुपर्ने मनासिव कारण देखिएमा नियन्त्रक आफैंले जाँचबुझ गर्न वा अन्य कुनै अधिकृत कर्मचारीद्वारा आवश्यक जाँचबुझ गराउन सक्नेछ। (२) उपदफा (१) बमोजिम जाँचबुझ पूरा नभएसम्मका लागि नियन्त्रकले प्रमाणीकरण निकायको इजाजतपत्र निलम्बन गर्न सक्नेछ। (३) उपदफा (२) बमोजिम निलम्बनमा परेको प्रमाणीकरण निकाय एक मात्र इजाजतपत्रवाला भएमा त्यसरी निलम्बनमा परेको अवधिभर सो सम्बन्धी काम नियन्त्रकको कार्यालयले गर्नेछ। (४) उपदफा (२) बमोजिम निलम्बनमा परेको प्रमाणीकरण निकायले प्रमाणीकरण कार्यमा प्रयोग गरेका हार्डवेयर, सफ्टवेयर, सूचना प्रविधि प्रणाली र सोसँग सम्बन्धित तथ्याङ्क नियन्त्रकलाई बुझाउनु पर्नेछ। (५) उपदफा (१) बमोजिम जाँचबुझ गर्दा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको पालना भएको नदेखिएमा नियन्त्रकले त्यस्तो प्रमाणीकरण निकायलाई आवश्यक निर्देशन दिन सक्नेछ र त्यस्तो निर्देशन पालना गर्नु प्रमाणीकरण निकायको कर्तव्य हुनेछ। (६) उपदफा (५) बमोजिमको निर्देशनको पालना गरेमा वा उपदफा (१) बमोजिम शङ्का गरिएको आरोप पुष्टि नभएमा उपदफा (२) बमोजिम गरिएको इजाजतपत्रको निलम्बन फुकुवा हुनेछ। (७) उपदफा (१) बमोजिमको जाँचबुझमा सहयोग पुऱ्याउनु प्रमाणीकरण निकायको कर्तव्य हुनेछ। (८) उपदफा (१) बमोजिम गरिने जाँचबुझको सम्बन्धमा अपनाउनु पर्ने कार्यविधि तोकिए बमोजिम हुनेछ।
२१.	२२	इजाजतपत्र रद्द गर्न सक्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) नियन्त्रकले यस ऐन बमोजिम जारी गरेको इजाजतपत्र देहायको अवस्थामा जुनसुकै बखत रद्द गर्न सक्नेछ :- (क) प्रमाणीकरण निकायले इजाजतपत्र प्राप्त गर्न वा नवीकरणको लागि निवेदन दिंदाको बखत झुट्टा वा गलत विवरण तथा कागजात दाखिला गरेको देखिएमा, (ख) प्रमाणीकरण निकायले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम

			अन्तर्गत कसूर ठहरिने कुनै काम गरेमा, (ग) यो ऐन वा यस ऐन अन्तर्गत बनेको नियम अन्तर्गत पूरा गर्नु पर्ने दायित्व प्रमाणीकरण निकायले पूरा नगरेमा वा (घ) यस ऐन बमोजिम नियन्त्रकले दिएको आदेश वा निर्देशनको उल्लङ्घन गरेमा। (२) उपदफा (१) बमोजिम नियन्त्रकले इजाजतपत्र रद्द गर्नु अघि प्रमाणीकरण निकायलाई सफाई पेश गर्ने मनासिब मौका दिनु पर्नेछ।
२२.	२३	निर्णयको जानकारी दिनुपर्ने	यस दफामा दफा २१ बमोजिम इजाजतपत्र निलम्बन वा दफा २२ बमोजिम इजाजतपत्र रद्द गर्ने गरी गरेको निर्णयको जानकारी नियन्त्रकले त्यस्तो प्रमाणीकरण निकायलाई लिखित रुपमा दिनु पर्नेछ र त्यस्तो सूचना कम्प्युटर प्रणालीमा राखी राष्ट्रिय दैनिक पत्रिकामा तथा विद्युतीय स्वरुपमा समेत प्रकाशन गर्नु पर्ने व्यवस्था गरिएको छ।
२३.	२४	प्रमाणपत्रको लागि निवेदन दिनु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र प्राप्त गर्न चाहने व्यक्तिले तोकिए बमोजिमको शुल्क तथा विवरण समेत संलग्न गरी प्रमाणीकरण निकाय समक्ष तोकिए बमोजिमको ढाँचामा निवेदन दिनु पर्नेछ। (२) उपदफा (१) बमोजिमको निवेदन पर्न आएमा प्रमाणीकरण निकायले आवश्यक छानबिन गरी निवेदन प्राप्त भएको एक महिना भित्र सो सम्बन्धमा निर्णय गरिसक्नु पर्नेछ। (३) उपदफा (२) बमोजिम प्रमाणीकरण निकायले प्रमाणपत्र जारी गर्ने निर्णय गरेमा पन्ध्र दिनभित्र आफ्नो हस्ताक्षर सहित प्रमाणपत्र जारी गर्नु पर्नेछ। (४) उपदफा (३) बमोजिम प्रमाणपत्र जारी नगर्ने निर्णय गरेमा सोको कारण सहितको सूचना पन्ध्र दिनभित्र निवेदकलाई दिनु पर्नेछ।
२४.	२५	प्रमाणपत्र जारी गर्न सक्ने	यस दफामा ऐन बमोजिम इजाजतपत्र प्राप्त गरेको प्रमाणीकरण निकाय र दफा १६ को उपदफा (३) बमोजिम मन्त्रालयले तोकेको सरकारी निकायले मात्र डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र जारी गर्न सक्ने व्यवस्था गरिएको छ।
२५.	२६	प्रमाणपत्र निलम्बन गर्न सक्ने	यस दफामा प्रमाणीकरण निकायले देहायका अवस्थामा प्रमाणपत्र प्राप्त व्यक्तिको प्रमाणपत्र निलम्बन गर्न सक्ने व्यवस्था गरिएको छः- (क) सार्वजनिक हित विपरीत हुने भई प्रमाणपत्र निलम्बन गर्नु पर्ने भएमा, (ख) प्रमाणपत्र प्राप्त व्यक्तिले यो ऐन वा यस ऐन अन्तर्गत बनेको नियममा लेखिएको कुराको पालना नगरेको कारणबाट त्यस्तो प्रमाणपत्र माथि भर

			पर्ने व्यक्तिका लागि उल्लेखनीय हानि नोक्सानी हुनसक्ने देखिएमा सो कुराको कारण खुलाई त्यस्तो प्रमाणपत्र निलम्बन गर्न नियन्त्रकले निर्देशन दिएमा।
२६.	२७	प्रमाणपत्र रद्द गर्न सक्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रमाणीकरण निकायले देहायका कुनै अवस्थामा प्रयोगकर्ताको प्रमाणपत्र रद्द गर्न सक्नेछः- (क) प्रमाणपत्र प्राप्त गर्ने प्रयोगकर्ता वा त्यस्तो प्रयोगकर्ताको तर्फबाट अख्तियारी पाएको व्यक्तिले सो प्रमाणपत्र रद्द गरी पाउनको लागि अनुरोध गरेमा, (ख) प्रमाणपत्र कायम राख्दा सार्वजनिक हित विपरीत हुने अवस्था भएमा, (ग) प्रयोगकर्ताको मृत्यु भएमा, (घ) प्रयोगकर्ता कुनै कम्पनी वा सङ्गठित संस्था भए त्यस्तो सङ्गठित संस्था वा कम्पनी प्रचलित कानून बमोजिम दामासाहीमा परेमा वा खारेजी वा विघटन भएमा, (ङ) प्रमाणपत्र जारी गर्दा पूरा गर्नु पर्ने सर्त पूरा नभएको प्रमाणित भएमा, (च) प्रमाणपत्रमा स्पष्ट पारिएको आधारभूत तथ्य झुट्ठा प्रमाणित भएमा, वा (छ) प्रमाणपत्रको विश्वासनीयतामा तात्विक रुपमा असर पर्ने गरी जोडी साँचो सिर्जना गर्न प्रयोग गरिएको साँचो वा सुरक्षण प्रणालीमा फेरबदल वा काँटछाँट गरिएमा। (२) उपदफा (१) बमोजिम प्रमाणपत्र रद्द गर्नु अघि सम्बन्धित प्रयोगकर्तालाई सफाइ पेश गर्ने मनासिब मौका दिनु पर्नेछ।
२७.	२८	प्रमाणपत्र निलम्बन वा रद्द गरिएको सूचना	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) दफा २६ बमोजिम प्रमाणपत्र निलम्बन वा दफा २७ बमोजिम प्रमाणपत्र रद्द गरिएकोमा त्यसरी प्रमाणपत्र निलम्बन गर्ने वा रद्द गर्ने प्रमाणीकरण निकायले सोको अभिलेख राखी त्यस्तो सूचना सार्वजनिक रुपमा प्रकाशन गर्नु पर्नेछ। (२) उपदफा (१) बमोजिम निलम्बन वा रद्द गरिएको सूचना यथाशीघ्र प्रयोगकर्तालाई दिनु पर्ने दायित्व प्रमाणीकरण निकायको हुनेछ।
२८.	२९	कार्यसम्पादन परीक्षण	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) नियन्त्रकले प्रत्येक वर्ष प्रमाणीकरण निकायको कार्यसम्पादनको

			परीक्षण गर्नु, गराउनु पर्नेछ। (२) उपदफा (१) बमोजिमको कार्यसम्पादन परीक्षण गर्नको लागि नियन्त्रकले सूचना तथा सञ्चार प्रविधि विषयमा कम्तीमा स्नातकोत्तर तह उत्तीर्ण गरेको र कम्प्युटर सुरक्षणको क्षेत्रमा कम्तीमा पाँच वर्षको अनुभव प्राप्त व्यक्तिलाई नियुक्त गर्न सक्नेछ। (३) उपदफा (२) बमोजिम कार्यसम्पादन परीक्षण गर्नको लागि नियुक्त व्यक्तिले सम्झौता भएको मितिले तीन महिनाभित्र कार्य सम्पन्न गरी नियन्त्रक समक्ष कार्यसम्पादन परीक्षणको प्रतिवेदन पेश गर्नु पर्नेछ। (४) उपदफा (१) बमोजिम गरिएको कार्यसम्पादन परीक्षणको प्रतिवेदन नियन्त्रकले आफ्नो कम्प्युटर तथ्याङ्क प्रणालीमा राखी विद्युतीय स्वरुपमा प्रकाशन गर्नु पर्नेछ। (५) नियन्त्रकले प्रमाणीकरण निकायको सेवाको स्तर निर्धारण गरी सोको सूचना सर्वसाधारणको जानकारीको लागि सार्वजनिक रुपमा प्रकाशन गर्नु पर्नेछ।
२९.	३०	कम्प्युटर र तथ्याङ्कमा पहुँच पाउने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले डिजिटल हस्ताक्षर सम्बन्धमा यो ऐन वा यस ऐन अन्तर्गत बनेको नियमको उल्लङ्घन गरेको छ भन्ने शङ्का गर्नु पर्ने मनासिव कारण भएमा 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 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।
३०.	३१	अभिलेख राख्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) यस ऐन बमोजिम जारी गरिएका सम्पूर्ण प्रमाणपत्रको अभिलेख नियन्त्रकले राख्नु पर्नेछ। (२) उपदफा (१) बमोजिमको अभिलेख सुरक्षित राख्ने प्रयोजनको लागि डिजिटल हस्ताक्षरको गोपनीयता र सुरक्षालाई सुनिश्चित गर्न नियन्त्रकले

			देहाय बमोजिमको कार्य गर्नु पर्नेछः- (क) कम्प्युटर सुरक्षण प्रणाली उपयोग गर्ने, (ख) डिजिटल हस्ताक्षरको गोपनीयता र अखण्डतालाई सुनिश्चित गर्न सुरक्षण कार्यविधि लागू गर्ने, र (ग) तोकिए बमोजिमको मापदण्डको पालना गर्ने। (३) नियन्त्रकले सार्वजनिक साँचोको विवरण एउटै कम्प्युटर प्रणालीमा आबद्ध हुने गरी कम्प्युटर तथ्याङ्क प्रणालीमा अद्यावधिक 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।
३१.	३२	विद्युतीय स्वरुपमा राख्न अनिवार्य नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) यस ऐनमा अन्यत्र जुनसुकै कुरा लेखिएको भए तापनि देहायका विषयहरू विद्युतीय स्वरुपमा राख्न अनिवार्य हुने छैनः- (क) विनिमेय अधिकारपत्र ऐन, २०३४ मा उल्लेख भए बमोजिमका विनिमेय अधिकारपत्रहरु, (ख) बकसपत्र, राजीनामा, बन्धकी, कबुलियतपत्र, ऋणपत्र वा त्यस्तै प्रकृतिका अचल सम्पत्तिको हक हस्तान्तरण गर्ने लिखतहरु, (ग) अचल सम्पत्ति उपर हक वा स्वामित्व जनाउने अन्य कुनै लिखतहरु, (घ) वारेसनामा, फिरादपत्र, प्रतिउत्तरपत्र वा अदालती काम कारबाहीमा प्रयोग हुने त्यस्तै प्रकृतिका अन्य लिखतहरु, (ङ) दावीपत्र, प्रतिदावीपत्र, प्रतिवादपत्र वा मध्यस्थताको कारबाहीमा लिखितरुपमा पेश गर्नुपर्ने त्यस्तै प्रकृतिका अन्य लिखतहरु। (२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी उपदफा (१) मा उल्लिखित विषयमा आवश्यकतानुसार थपघट गर्न सक्नेछ।
३२.	३३	विवरण वा कागजात दाखिला गर्नु पर्ने	यस दफामा यो ऐन वा यस ऐन अन्तर्गत बनेको नियम बमोजिम नियन्त्रक वा प्रमाणीकरण निकाय समक्ष कुनै विवरण, कागजात र प्रतिवेदन दाखिला गर्नु पर्ने जिम्मेवारी भएको व्यक्तिले तोकिएको म्यादभित्र त्यस्तो विवरण, कागजात र प्रतिवेदन दाखिला गर्नु पर्ने व्यवस्था गरिएको छ।

३३.	३४	अधिकार प्रत्यायोजन गर्न सक्ने	यस दफामा नियन्त्रकले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम बमोजिम आफूलाई प्राप्त अधिकार मध्ये न्यायिक अधिकार बाहेकका अन्य अधिकार आफ्नो मातहतका कुनै अधिकृत कर्मचारीले प्रयोग गर्ने गरी प्रत्यायोजन गर्न सक्ने व्यवस्था गरिएको छ।
३४.	३५	जोडी साँचो सिर्जना गर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रमाणीकरण निकायबाट जारी गरिएको र ग्राहकद्वारा स्वीकार गरिएको प्रमाणपत्रमा सूचीकृत गरिनु पर्ने सार्वजनिक साँचो समावेश भएको जोडी साँचो ग्राहकले नै सिर्जना गर्नु पर्ने भएमा ग्राहकले त्यस्तो जोडी साँचो सिर्जना गर्दा सुरक्षित एसिमेट्रिक क्रिप्टो सिस्टमको प्रयोग गर्नु पर्नेछ । (२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि जोडी साँचो सिर्जना गर्न प्रयोग गर्नु पर्ने सुरक्षण प्रणालीको सम्बन्धमा प्रयोगकर्ता र प्रमाणीकरण निकायका बिचमा 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।
३५.	३६	प्रमाणपत्र स्वीकार गरेको मानिने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (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 प्रयोगकर्ताले प्रमाणपत्रलाई स्वीकार गरेको भएमा सो कारणबाट प्रयोगकर्ताले प्रमाणपत्रमा उल्लेख भएको कुनै सूचना माथि भर पर्ने व्यक्तिलाई देहायका कुराको 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 तथ्य सत्य भएको, र (ग) प्रमाणपत्रमा उल्लेख भएका सूचना सत्य र दुरुस्त भएको।

३६.	३७	निजी साँचोलाई सुरक्षित राख्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रत्येक प्रयोगकर्ताले आफूले प्राप्त गरेको प्रमाणपत्रमा सूचीकृत गरिएको सार्वजनिक साँचोसँग सम्बन्धित निजी साँचोलाई सुरक्षित राख्नु पर्नेछ। डिजिटल हस्ताक्षर सिर्जना गर्ने अख्तियारी नपाएको कुनै पनि व्यक्तिलाई त्यस्तो साँचो बारे जानकारी नहुने गरी आवश्यक सबै उपाय अवलम्बन गर्नु पर्नेछ। (२) प्रयोगकर्ताको निजी साँचोको सम्बन्धमा कसैलाई 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 यथाशीघ्र प्रमाणपत्र निलम्बन गर्नु पर्नेछ। (३) यस ऐन बमोजिम प्रमाणपत्र निलम्बन भएमा त्यस्तो निलम्बन अवधिभर निजी साँचो सुरक्षित राख्नु प्रयोगकर्ताको कर्तव्य हुनेछ।
३७.	३८	निजी साँचो नियन्त्रक समक्ष दाखिला गर्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) नेपालको सार्वभौमिकता वा अखण्डताको रक्षा गर्न वा मित्रराष्ट्रसँगको 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) बमोजिम दाखिला भएको निजी साँचो बारे नियन्त्रकले अनधिकृत व्यक्तिलाई जानकारी गराउन हुँदैन।
३८.	३९	डोमेन नाम, व्यवस्थापन तथा नियमन	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) डोमेन नाम, सोको व्यवस्थापन तथा नियमन विभागले गर्नेछ। (२) डोमेन नाम सञ्चालनलाई भरपर्दो र सुरक्षित बनाउनको लागि विभागले डोमेन नाम सञ्चालकलाई आवश्यक निर्देशन दिन सक्नेछ।
३९.	४०	डोमेन नाम दर्ता गर्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कुनै व्यक्ति वा संस्थाले एनपी डोमेनमा नाम दर्ता गराउँदा विभागले तोकेको संस्थामा 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 वा मिल्दोजुल्दो हुने गरी डोमेन नाम दर्ता गर्न वा गराउन हुँदैन। (४) सरकारी निकायले आफ्नो कार्यालयको डोमेन नाम गभर्मेन्ट डट एनपी (gov.np) अन्तर्गत दर्ता गर्नु पर्नेछ। (५) उपदफा (१) बमोजिम दर्ता भएको डोमेन नाम प्रत्येक दुई वर्षमा तोकिए बमोजिमको दस्तुर बुझाई नवीकरण गर्नु पर्नेछ। तर सरकारी निकायको डोमेन नाम नवीकरण गर्नु पर्ने छैन। (६) यो ऐन प्रारम्भ हुँदाका वखत सञ्चालनमा रहेका डोमेन नाम यो ऐन प्रारम्भ भएको मितिले छ महिनाभित्र यस ऐन बमोजिम दर्ता गर्नु पर्नेछ।
४०.	४१	डोमेन नाम सुरक्षित रहने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) देहाय बमोजिमका नाम दोस्रो र तेस्रो तहका डोमेन नामको लागि सुरक्षित रहनेछन्ः- (क) प्रचलित कानून बमोजिम कुनै कम्पनीको नाममा दर्ता गरिएको व्यापारिक नाम, (ख) भौगोलिक वा पर्यटकीय स्थलको नाम, (ग) पुरातात्त्विक वा धार्मिक महत्त्वको नाम, (घ) राष्ट्रियरुपमा ख्याति प्राप्त व्यक्तिका नाम, (ङ) सरकारी संस्थाको नाम, (च) अन्तर्राष्ट्रिय गैरसरकारी संस्थाको नाम, (छ) नेपाल सरकारले तोकेका अन्य नाम। (२) उपदफा (१) को खण्ड (क), (घ) र (ङ) बमोजिमका डोमेन नाम सम्बन्धित संस्थाले मात्र र अन्य नाम मन्त्रालयले तोकेको निकायको स्वीकृति लिई जो कसैले प्रयोग गर्न पाउनेछ। (३) उपदफा (१) बमोजिमका सुरक्षित नामसँग मिल्दोजुल्दो हुने गरी वा उक्त नामको महत्वलाई अवमूल्यन गर्ने गरी डोमेन नाम दर्ता गर्न वा गराउन हुँदैन।
४१.	४२	अनधिकृत रुपमा डोमेन नाम प्रणाली सञ्चालन गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले यो ऐन वा यस ऐन अन्तर्गत बनेको नियम विपरीत अनधिकृत रुपले डोमेन नाम प्रणाली सञ्चालन गर्न वा गराउन हुँदैन। (२) उपदफा (१) बमोजिमको कार्य गरेमा विभागले एक लाख

			रुपैयाँसम्म जरिबाना गर्न सक्नेछ।
४२.	४३	डाटा सेन्टर तथा क्लाउड सेवा सञ्चालन गर्न इजाजतपत्र लिनु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) नेपालभित्र डाटा सेन्टर, क्लाउड वा दुवै सेवा सञ्चालन गर्न चाहने संस्थाले विभागबाट इजाजतपत्र लिनु पर्नेछ। तर कुनै संस्थाले आफ्नो निजी प्रयोजनको लागि मात्र सञ्चालन गर्ने डाटा सेन्टर, क्लाउड वा दुवै सेवाको लागि इजाजतपत्र लिनु पर्ने छैन। (२) उपदफा (१) बमोजिम इजाजतपत्र लिन विभागमा निवेदन दिनु पर्नेछ। (३) उपदफा (२) बमोजिम निवेदन प्राप्त भएपछि जाँचवुझ गर्दा डाटा सेन्टर, क्लाउड वा दुवै सेवा सञ्चालन गर्न मापदण्ड पूरा गरेको पाइएमा विभागले इजाजपत्र दिनेछ। (४) यो ऐन प्रारम्भ हुँदाका बखत सञ्चालनमा रहेका डाटा सेन्टर, क्लाउड वा दुवै सेवा प्रदायकले यो ऐन प्रारम्भ भएको एक वर्षभित्र यस दफा बमोजिमको इजाजतपत्र लिनु पर्नेछ। (५) उपदफा (३) र (४) बमोजिम इजाजतपत्र प्राप्त संस्थाले वार्षिक रुपमा अद्यावधिक विवरण विभागमा पेश गर्नु पर्नेछ र विभागले वर्षको कम्तीमा दुई पटक अनुगमन गर्नु पर्नेछ। (६) उपदफा (३) र (४) बमोजिमको इजाजतपत्र प्राप्त व्यक्तिले इजाजतपत्रको नवीकरण गर्न चाहेमा प्रत्येक दुई वर्षमा नवीकरण गर्नु पर्नेछ।
४३.	४४	डाटा सेन्टर वा क्लाउडमा सूचना प्रणाली राख्न सक्नेः	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) सरकारी निकायले तोकिए बाहेकका सूचना प्रणाली दफा ४३ बमोजिम इजाजतपत्र प्राप्त डाटा सेन्टर वा क्लाउडमा राखी सञ्चालन गर्न सक्नेछ। (२) डाटा सेन्टर वा क्लाउडमा कम्प्युटर प्रणाली राख्ने सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।
४४.	४५	इजाजतपत्र नलिई डाटा सेन्टर, क्लाउड वा दुवै सञ्चालन गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले यस ऐन बमोजिम इजाजतपत्र नलिई डाटा सेन्टर, क्लाउड वा दुवै सञ्चालन गर्न हुँदैन। (२) उपदफा (१) बमोजिम इजाजतपत्र नलिई डाटा सेन्टर, क्लाउड वा

			दुवै सञ्चालन गरेमा विभागले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।
४५.	४६	केन्द्रको स्थापना	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) साइबर सुरक्षाको चुनौतिको अनुगमन र प्रतिकार्य समेतको लागि राष्ट्रिय साइबर सुरक्षा केन्द्र रहनेछ। (२) केन्द्रको कार्यालय काठमाडौं उपत्यकामा रहनेछ । (३) केन्द्रको प्रमुखको रुपमा कार्य गर्न मन्त्रालयले सहसचिवस्तरको कर्मचारीलाई तोक्न सक्नेछ । (४) केन्द्रको काम सुचारु रुपले सञ्चालन गर्न आवश्यक सङ्ख्यामा कर्मचारी रहनेछन्।
४६.	४७	केन्द्रको काम, कर्तव्य र अधिकार	यस दफामा यस ऐनमा अन्यत्र उल्लिखित काम, कर्तव्य र अधिकारको अतिरिक्त केन्द्रको काम, कर्तव्य र अधिकार देहाय बमोजिम हुने व्यवस्था गरिएको छः- (क) साइबर सुरक्षा जोखिमको अनुगमन तथा विश्लेषण गर्ने, (ख) संवेदनशील सूचना पूर्वाधारको चौविसै घण्टा अनुगमन गर्ने तथा साइबर घटना तथा जोखिम मूल्याङ्कन गर्ने, (ग) राष्ट्रिय सुरक्षा, प्रतिरक्षा, अर्थतन्त्र, जनस्वास्थ्य, सार्वजनिक शान्ति र व्यवस्था वा सार्वजनिक सुरक्षा वा अत्यावश्यक सेवामा पार्न सक्ने साइबर सुरक्षाका घटनाको प्रतिकार्य गर्ने, (घ) संवेदनशील सूचना पूर्वाधारको पहिचान गरी निर्देशक समिति समक्ष पेश गर्ने, (ङ) संवेदनशील सूचना पूर्वाधारका धनीले अवलम्बन गरेको साइबर सुरक्षा अभ्यासको अनुगमन गर्ने, (च) साइबर सुरक्षा सम्बन्धी प्राविधिक मापदण्ड तयार गरी निर्देशक समिति समक्ष पेश गर्ने, (छ) साइबर सुरक्षा सम्बन्धी डिजिटल फोरेन्सिक ल्याव सञ्चालन गर्ने, (ज) साइबर सुरक्षा सेवा प्रदायक अनुमतिपत्रको सर्त तथा मापदण्ड तर्जुमा गरी निर्देशक समिति समक्ष पेस गर्ने, (झ) साइबर सुरक्षाको घटनाका सम्बन्धमा अन्य मुलुकका कम्प्युटर आपतकालीन प्रतिकार्य समूहसँग समन्वय र सहकार्य गर्ने, (ञ) साइबर सुरक्षा सम्बन्धी प्रविधिको अध्ययन, अनुसन्धान तथा

			विकासलाई प्रोत्साहन गर्ने तथा आवश्यकता अनुसार त्यस्ता कार्य गर्न विश्वविद्यालय वा सम्बन्धित सङ्घ संस्थासँग समन्वय र सहकार्य गर्ने, (ट) साइबर चुनौतीको पहिचान, रोकथाम, प्रतिक्रिया तथा पुनर्लाभ लगायतका कामको साइबर सुरक्षा सेवा प्रदायकको रुपमा सूचीकरण गर्ने, (ठ) कम्प्युटर वा कम्प्युटर प्रणालीको साइबर सुरक्षा निरीक्षण गर्ने, (ड) आकस्मिक रुपमा आइपर्ने साइबर जोखिमलाई समाधान गर्नको लागि प्राविधिक जनशक्ति सहितको आकस्मिक सहायता समूहको गठन गर्ने, (ढ) मानवीय वा प्राकृतिक कारणले हानी नोक्सानी पुगी राष्ट्रिय सुरक्षा, अर्थ व्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य वा सार्वजनिक सुरक्षासँग सम्बन्धित सूचना प्रविधि प्रणाली बन्द भएमा यथाशीघ्र सो प्रणालीलाई पुनः सञ्चालनमा ल्याउन सहयोग गर्ने, (ण) सूचना प्रविधि र साइबर सुरक्षा सम्बन्धी घटनाको अध्ययन तथा विश्लेषण गरी सम्बन्धित निकाय वा व्यक्तिलाई जानकारी गराउने तथा सोको समाधानको लागि सहजीकरण गर्ने, (त) आवश्यकता अनुसार विषयगत तथा क्षेत्रगत सहायता समूह गठन गर्ने र सो समूहको काम कारबाहीको अनुगमन गर्ने, गराउने, (थ) विषयगत तथा क्षेत्रगत सहायता समूहको गठन, कार्यक्षेत्र र सञ्चालन सम्बन्धी कार्यविधि बनाई निर्देशक समिति समक्ष पेश गर्ने, र (द) साइबर सुरक्षा सम्बन्धमा आवश्यक अन्य कार्य गर्ने गराउने।
४७.	४८	केन्द्रले निर्देशन दिन सक्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) केन्द्रले यो ऐन बमोजिम कार्य गर्न संवेदनशील सूचना पूर्वाधारका धनी, अनुमतिपत्र प्राप्त सेवा प्रदायक तथा साइबर सुरक्षा परीक्षकलाई निर्देशन दिन सक्नेछ र त्यस्तो निर्देशनको पालना गर्नु सम्बन्धित संवेदनशील सूचना पूर्वाधारका धनी, अनुमतिपत्र प्राप्त सेवा प्रदायक तथा साइबर सुरक्षा परीक्षकको कर्तव्य हुनेछ। (२) उपदफा (१) बमोजिमको निर्देशन पालना नगरेमा केन्द्रले एक लाख रुपैयाँसम्म जरिबाना गर्नेछ।
४८.	४९	वार्षिक प्रतिवेदन	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) केन्द्रले प्रत्येक आर्थिक वर्ष समाप्त भएको मितिले तीन महिना भित्र

			आफूले सम्पादन गरेको काम कारबाहीको प्रतिवेदन तयार गरी मन्त्रालय समक्ष पेश गर्नु पर्नेछ। (२) उपदफा (१) बमोजिमको प्रतिवेदनमा अन्य कुराका अतिरिक्त केन्द्रले प्राप्त गरेको बजेट तथा कार्यक्रम र सो कार्यक्रम सञ्चालन गर्दा हुन गएको खर्च, मुख्य मुख्य कामको विवरण तथा उपलब्धि र भविष्यमा गर्नु पर्ने सुधार समेतका विषय समावेश गर्नु पर्नेछ।
४९.	५०	साइबर सुरक्षा सेवा प्रदान गर्न सूचीकृत हुनु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) साइबर सुरक्षा सेवा प्रदान गर्न चाहने व्यक्ति, कम्पनी वा संस्था साइबर सुरक्षा सेवा प्रदायकको रुपमा केन्द्रमा सूचीकृत हुनु पर्नेछ। (२) सार्वजनिक संस्थाले साइबर सुरक्षा सेवा लिँदा उपदफा (१) बमोजिम सूचीकृत साइबर सुरक्षा सेवा प्रदायकबाट लिनु पर्नेछ।
५०.	५१	सूचीकृत हुन निवेदन दिने	यस दफामा दफा ५० बमोजिम सूचीकृत हुन चाहने व्यक्ति, कम्पनी वा संस्थाले देहायको कागजात संलग्न गरी तोकिए बमोजिमको ढाँचामा केन्द्रमा निवेदन दिनु पर्ने व्यवस्था गरिएको छः- (क) कम्पनी वा संस्थाको प्रबन्धपत्र र नियमावली, (ख) कम्पनी वा संस्था दर्ताको प्रमाणपत्र, (ग) कम्पनीको मुल्य अभिवृद्धि कर वा स्थायी लेखा नम्बर दर्ताको प्रमाणपत्र, (घ) कम्पनी अद्यावधिक भएको पत्र, (ङ) अघिल्लो आर्थिक वर्षको कर चुक्ता प्रमाणपत्र, (च) कम्पनी वा संस्थाको सञ्चालक समितिको विवरण, (छ) व्यक्तिको हकमा नेपाली नागरिकताको प्रमाणपत्र वा राष्ट्रिय परिचयपत्रको प्रतिलिपि।
५१.	५२	सूचीकृत गर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) दफा ५१ 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 साइबर सुरक्षा सेवा प्रदायकको रुपमा सूचीकृत गर्नेछ। (२) सूचीकरणको मान्य अवधि सूचीकृत भएको मितिले तीन वर्षको

			हुनेछ। (३) यस ऐन बमोजिम सूचीकृत व्यक्ति, कम्पनी वा संस्थाले साइबर सुरक्षा सम्बन्धी सेवा प्रदान गरेको विवरणको वार्षिक रुपमा तोकिए बमोजिमको ढाँचामा अभिलेख राख्नु पर्नेछ ।
५२.	५३	अद्यावधिक र अभिलेख	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) सूचीकृत व्यक्तिले सूची अद्यावधिक गर्न चाहेमा दफा ५२ को उपदफा (२) बमोजिमको अवधि समाप्त हुनु भन्दा कम्तीमा तीस दिन अघि अद्यावधिक गर्नको लागि देहायका कागजात संलग्न गरी केन्द्रमा निवेदन दिनु पर्नेछः- (क) सूचीकृत संस्थाले प्रदान गरेको साइबर सुरक्षा सेवाको वार्षिक विवरण, (ख) कम्पनी वा संस्थाको हकमा कर चुक्ता प्रमाणपत्र र कम्पनी अद्यावधिक भएको पत्र। (२) उपदफा (१) बमोजिम प्राप्त निवेदन उपर जाँचबुझ गर्दा निवेदकले सूचीकृत गर्दाको बखत तोकिएको सर्त पालना गरेको देखिएमा केन्द्रले दुई वर्षको लागि अद्यावधिक गर्न सक्नेछ। (३) केन्द्रले सूचीकृत साइबर सुरक्षा सेवा प्रदायकको अभिलेख राख्नु पर्नेछ।
५३.	५४	संवेदनशील सूचना पूर्वाधार तोक्ने	यस दफामा केन्द्रको सिफारिसमा नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशित गरी संवेदनशील सूचना पूर्वाधार तोक्न सक्ने व्यवस्था गरिएको छ।
५४.	५५	संवेदनशील सूचना पूर्वाधार सम्बन्धी जानकारी माग गर्न सक्नेः	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) केन्द्रले संवेदनशील सूचना पूर्वाधारका धनीसँग देहायका विषयमा जानकारी माग गर्न सक्नेछः- (क) संवेदनशील सूचना पूर्वाधारको डिजाइन, कन्फिगुरेसन तथा सुरक्षा सम्बन्धी जानकारी, (ख) संवेदनशील सूचना पूर्वाधारसँग जोडिएका वा सूचना आदानप्रदान गर्ने कम्प्युटर वा कम्प्युटर प्रणालीको डिजाइन, कन्फिगुरेसन तथा सुरक्षा र सोसँग सम्बन्धित कम्प्युटर प्रणालीको सञ्चालन सम्बन्धी जानकारी। (२) उपदफा (१) बमोजिम माग गरिएको जानकारी उपलब्ध गराउनु

			सूचना पूर्वाधारका धनीको कर्तव्य हुनेछ। तर प्रचलित नेपाल कानूनले त्यस्तो जानकारी दिन रोक लगाएको भएमा यस दफा बमोजिम जानकारी दिन बाध्य गरेको मानिने छैन।
५५.	५६	साइबर सुरक्षा अनुगमन र परीक्षण	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) संवेदनशील सूचना पूर्वाधारको धनीले कम्तीमा वर्षको एक पटक दफा ५९ बमोजिमको परीक्षकबाट संवेदनशील सूचना पूर्वाधारको सुरक्षा परीक्षण गराई उक्त परीक्षण प्रतिवेदन केन्द्र समक्ष पेश गर्नु पर्नेछ। (२) उपदफा (१) बमोजिम साइबर सुरक्षा परीक्षण सन्तोषजनक नदेखिएमा केन्द्रले पुनः परीक्षण गराउन निर्देशन दिन सक्नेछ। त्यस्तो परीक्षणको प्रतिवेदन संवेदनशील सूचना पूर्वाधार धनीले केन्द्र समक्ष पेश गर्नु पर्नेछ। (३) केन्द्रले साइबर सुरक्षामा देखिएका कमी कमजोरी सुधार गर्न संवेदनशील सूचना पूर्वाधारका धनीलाई लेखी पठाउन सक्नेछ र त्यसरी लेखी आएमा संवेदनशील सूचना पूर्वाधारका धनीले आफ्नो कम्प्युटर वा कम्प्युटर प्रणालीमा देखिएका त्यस्ता कमी कमजोरी तत्कालै हटाउनु पर्नेछ। (४) केन्द्रले संवेदनशील सूचना पूर्वाधारको अनुगमन गर्ने व्यवस्था गर्नेछ।
५६.	५७	साइबर सुरक्षाका घटनाको जानकारी गराउनु पर्ने	यस दफामा संवेदनशील सूचना पूर्वाधारका धनीले साइबर सुरक्षाको घटना घटेमा त्यस्तो घटना लगत्तै देहायका विषयमा केन्द्रलाई जानकारी गराउनु पर्ने व्यवस्था गरिएको छः- (क) संवेदनशील सूचना पूर्वाधार प्रणालीको धनीले आफूले सञ्चालन गरेको संवेदनशील पूर्वाधार प्रणालीसँग सञ्चार आदानप्रदान गर्ने गरी जोडिएको कुनै कम्प्युटर वा कम्प्युटर प्रणालीसँग सम्बन्धित साइबर सुरक्षा घटना, (ख) संवेदनशील सूचना पूर्वाधारसँग सम्बन्धित साइबर सुरक्षा सम्बन्धी अन्य कुनै किसिमको घटना।
५७.	५८	साइबर सुरक्षा अभ्यास गराउनु पर्ने	यस दफामा संवेदनशील सूचना पूर्वाधारका धनीले कुनै साइबर सुरक्षा घटनामा प्रतिक्रिया गर्न तत्पर अवस्थामा राखे नराखेको परीक्षण गर्न समय समयमा साइबर सुरक्षा अभ्यास गर्नु पर्ने व्यवस्था गरिएको छ।
५८.	५९	साइबर सुरक्षा परीक्षक सूचीकृत हुनुपर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) साइबर सुरक्षा परीक्षण गर्न चाहने व्यक्ति वा संस्थाले साइबर सुरक्षा परीक्षकको रुपमा 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 प्रत्येक बर्ष सूची अद्यावधिक गर्नु पर्नेछ। (४) साइबर सुरक्षा परीक्षकको रुपमा सूचीकृत हुन केन्द्रमा देहायका कागजात पेश गर्नु पर्नेछः- (क) संस्था दर्ताको प्रमाणपत्र, (ख) मूल्य अभिवृद्धि कर वा स्थायी लेखा नम्बर दर्ताको प्रमाणपत्र, (ग) करचुक्ताको प्रमाणपत्र, र (घ) सम्बन्धित व्यक्तिको हकमा नेपाली नागरिकताको प्रमाणपत्र वा राष्ट्रिय परिचयपत्र, शैक्षिक प्रमाणपत्र, तालिमको प्रमाणपत्र, व्यवसायिक प्रमाणपत्रको प्रतिलिपि। (५) सूचीकरणका लागि आवश्यक योग्यता, मापदण्ड र साइबर सुरक्षा परीक्षकको कार्य तोकिए बमोजिमको हुनेछ। (६) उपदफा (१) बमोजिम सूचीकृत नभइ कुनै व्यक्ति वा संस्थाले साइबर सुरक्षा परीक्षकको रुपमा काम गरेमा केन्द्रले पचास हजार रुपैयाँसम्म जरिबाना गर्न सक्नेछ।
५९.	६०	सूचीकृत गर्नु पर्ने	यस दफामा केन्द्रले तोकेको साइबर सुरक्षासँग सम्बन्धित हार्डवेयर उत्पादन र आपूर्ति सम्बन्धी कार्य गर्ने व्यक्ति, साइबर सुरक्षासँग सम्बन्धित भनी केन्द्रले तोकेको सफ्टवेयर विकास र आपूर्ति सम्बन्धी कार्य गर्ने व्यक्ति र सो हार्डवेयर तथा सफ्टवेयर सञ्चालनका सम्बन्धमा परामर्श तथा अन्य सेवा उपलब्ध गर्ने व्यक्ति तोकिए बमोजिम केन्द्रमा सूचीकृत हुनु पर्ने व्यवस्था गरिएको छ।
६०	६१	वैयक्तिक विवरणको सङ्कलन	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले वैयक्तिक विवरण सङ्कलन गर्नु परेमा सो विवरण कुन प्रयोजनको लागि आवश्यक परेको हो त्यस्तो प्रयोजन खुलाई सम्बन्धित व्यक्तिसँग अनुमति लिनु पर्नेछ। (२) सूचना प्रविधि प्रणालीमा रहेका कुनै व्यक्तिको वैयक्तिक विवरण सङ्कलन गर्दा खुलाईएको प्रयोजन बाहेक अन्य प्रयोजनका लागि प्रयोग, प्रसार तथा आदानप्रदान गर्न पाईने छैन।

			तर सम्बन्धित व्यक्तिको स्वीकृतिमा अन्य प्रयोजनका लागि प्रयोग तथा प्रसार गर्न बाधा परेको मानिने छैन। (३) कुनै खास प्रयोजनका लागि कानून बमोजिम सङ्कलन तथा सञ्चय गरिएको वैयक्तिक सूचना सङ्कलन तथा सञ्चयको प्रयोजन समाप्त भएको पैंतिस दिनभित्र सम्बन्धित व्यक्तिलाई प्रत्याभूत हुने गरी नष्ट गर्नु पर्नेछ।
६१.	६२	सूचना सुरक्षाको सुनिश्चितता गर्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रशोधनकर्ता, सञ्चयकर्ता र सेवा प्रदायकले विद्युतीय स्वरुपमा रहेका सूचनाको आदानप्रदान, प्रशोधन तथा सञ्चय गर्दा निर्धारित मापदण्डको आधारमा सुरक्षाको सुनिश्चितता गर्नु पर्नेछ। (२) सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्य सम्बन्धी सेवा प्रदाय संस्थाले तोकिएको विवरण इन्क्रिप्ट गरी सुरक्षित राख्नु पर्नेछ। (३) सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्य सम्बन्धी सेवा प्रदायक संस्थाले विवरण तथा सूचना प्रशोधन तथा भण्डारण गर्दा नेपाल बाहिर नजाने गरी सुरक्षित गर्नु पर्नेछ। (४) सूचना सुरक्षा सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।
६२.	६३	सुरक्षा मापदण्ड अवलम्बन गर्नु पर्ने	यस दफामा सरकारी निकाय तथा सार्वजनिक संस्थाले कम्प्युटर तथा सूचना प्रणालीको प्रयोग गर्दा सुरक्षा मापदण्ड अवलम्बन गर्नु पर्नेछ।
६३.	६४	सेवा प्रदायकले दायित्व ब्यहोर्नु नपर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रचलित कानूनमा जुनसुकै कुरा लेखिएको भए तापनि देहायको अवस्थामा सेवा प्रदायकले कुनै तेस्रो पक्षको सूचना वा तथ्याङ्क वा लिङ्कमा पहुँच उपलब्ध गराएको कारणबाट मात्र उक्त सूचना वा तथ्याङ्क वा लिङ्कमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणको सम्बन्धमा उत्पन्न हुने कुनै दायित्व व्यहोर्नु पर्ने छैनः- (क) सूचना, तथ्याङ्क वा लिङ्कमा पहुँच पुऱ्याउने कार्यमा मात्र सीमित रहेको भएमा, (ख) आफैं प्रसारण नगरेको, प्रसारणको उपभोगकर्ता आफैं चयन नगरेको र प्रसारणमा रहेको सूचना छनौट तथा परिवर्तन नगरेको भएमा, (ग) आफ्नो सूचना प्रणालीमा भण्डारण गरेको कुनै खास सूचना गैरकानूनी रहेको भनी कुनै सम्बन्धित सार्वजनिक निकाय वा अदालतबाट त्यस्तो

			सूचना सामग्री हटाउन वा त्यस्ता सूचनामा पहुँच निष्क्रीय पार्न प्राप्त आदेश बमोजिम सेवा प्रदायकले सूचना सामग्री यथाशीघ्र हटाएमा वा पहुँच निष्क्रीय बनाएमा, (घ) नियामक निकायको सम्बन्धित निर्देशन पालना गरेको भएमा। (२) उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि कुनै सूचना, तथ्याङ्क वा लिङ्कमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणले प्रचलित कानूनको उल्लङ्घन गरेमा वा कुनै गैरकानूनी कार्य गर्न दुरुत्साहन वा सहयोग गरेमा सेवा प्रदायक त्यस्तो दायित्वबाट मुक्त हुने छैन।
६४.	६५	सूचना सुरक्षित राख्नु पर्ने	यस दफामा सेवा प्रदायकले सेवा प्रयोग सम्बन्धी तोकिए बमोजिमका सूचना तोकिएको अवधिसम्म सुरक्षित राख्नु पर्ने व्यवस्था गरिएको छ ।
६५.	६६	निर्देशक समितिको गठन	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) सूचना प्रविधि तथा साइबर सुरक्षाको क्षेत्रमा नीतिगत मार्गदर्शन गर्न देहाय बमोजिमको सूचना प्रविधि तथा साइबर सुरक्षा निर्देशक समिति रहनेछः- (क) सञ्चार तथा सूचना प्रविधि मन्त्री -अध्यक्ष (ख) गभर्नर, नेपाल राष्ट्र बैङ्क -सदस्य (ग) सचिव, प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय -सदस्य (घ) सचिव, गृह मन्त्रालय -सदस्य (ङ) सचिव, मन्त्रालय -सदस्य (च) अध्यक्ष, नेपाल दूरसञ्चार प्राधिकरण -सदस्य (छ) सूचना प्रविधि वा साइबर सुरक्षाको क्षेत्रमा स्नाकोत्तर उपाधि हासिल गरी कम्तीमा पन्ध्र वर्ष काम गरी ख्यातिप्राप्त गरेका व्यक्तिमध्येबाट मन्त्रालयले मनोनयन गरेको कम्तीमा एकजना महिला सहित दुई जना -सदस्य (ज) महानिर्देशक, राष्ट्रिय साइबर सुरक्षा केन्द्र -सदस्य (झ) सहसचिव (प्राविधिक), मन्त्रालय -सदस्य-सचिव (२) उपदफा (१) को खण्ड (ञ) बमोजिमका मनोनित सदस्यको पदावधि दुई वर्षको हुनेछ। (३) उपदफा (२) मा जुनसुकै कुरा लेखिएको भए तापनि मनोनित सदस्यको कार्यसम्पादन सन्तोषजनक नभएमा वा पद अनुकूलको आचरण पालना

			नगरेमा मन्त्रालयले त्यस्तो सदस्यलाई जुनसुकै बखत पदबाट हटाउन सक्नेछ। तर त्यसरी पदबाट हटाउँदा निजलाई सफाइ पेश गर्ने मनासिब मौका दिनु पर्नेछ।
६६.	६७	निर्देशक समितिको काम, कर्तव्य र अधिकार	यस दफामा निर्देशक समितिको काम, कर्तव्य र अधिकार देहाय बमोजिम हुने व्यवस्था गरिएको छः- (क) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी नीति तथा कानूनमा सुधार गर्नका लागि नेपाल सरकार समक्ष सिफारिस गर्ने, (ख) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी प्राविधिक मापदण्ड स्वीकृतिको लागि नेपाल सरकार, मन्त्रिपरिषद् समक्ष पेश गर्ने, (ग) सूचना प्रविधि प्रणाली र पूर्वाधारको एकरुपता तथा अन्तरआवद्धताको लागि सहजीकरण गर्ने, (घ) विद्युतीय सुशासनको लागि सम्बन्धित निकायलाई उत्तरदायी बनाउने तथा शासन प्रणालीको तीनै तहसम्म विद्युतीय शासन विस्तार गर्न सहजीकरण गर्ने, (ङ) सूचना प्रविधिको क्षेत्रमा रोजगारीका अवसर विस्तार गर्न सरकारी तथा निजी क्षेत्रको सहकार्य तथा साझेदारीलाई प्रवर्द्धन गर्न सहजीकरण गर्ने, (च) कृत्रिम बौद्धिकता (ए.आई.) को अनुसन्धान, विकास तथा प्रयोगलाई प्रोत्साहन गर्ने, (छ) सूचना प्रविधि, साइबर सुरक्षा तथा कृत्रिम बौद्धिकताको प्रयोगको सम्बन्धमा प्रदेश, स्थानीय तह तथा अन्य सम्बद्ध निकाय बिच आवश्यक समन्वय गर्ने, (ज) केन्द्रको सिफारिसमा संवेदनशील सूचना पूर्वाधारको धनीले पालना गर्नु पर्ने सर्त, सुरक्षाको उपायका सम्बन्धमा निर्देशन दिने वा सो सम्बन्धी आवश्यक मापदण्ड स्वीकृत गर्ने, र (झ) सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी आवश्यक अन्य कार्य गर्ने।
६७.	६८	निर्देशक समितिको बैठक	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) निर्देशक समितिको बैठक आवश्यकतानुसार बस्नेछ। (२) निर्देशक समितिको बैठक सो समितिको अध्यक्षले तोकेको मिति, समय र स्थानमा बस्नेछ।

			(३) निर्देशक समितिको बैठकको अध्यक्षता समितिको अध्यक्षले गर्नेछ। (४) निर्देशक समितिको बैठकमा बहुमतको राय मान्य हुनेछ र मत बराबर भएमा बैठकमा अध्यक्षता गर्ने व्यक्तिले निर्णायक मत दिनेछ। (५) निर्देशक समितिको बैठकको निर्णय बैठकमा उपस्थित सबै सदस्यबाट प्रमाणित गरी अभिलेख राख्नु पर्नेछ। (६) निर्देशक समितिले आवश्यकता अनुसार सम्बन्धित विषयको विशेषज्ञलाई समितिको बैठकमा आमन्त्रण गर्न सक्नेछ।
६८.	६९	विद्युतीय माध्यमबाट सेवा प्रवाह विद्युतीय माध्यमबाट सार्वजनिक सेवा प्रदान गर्न सकिने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) सरकारी निकाय तथा सार्वजनिक संस्थाले आफूले प्रदान गर्ने सार्वजनिक सेवा विद्युतीय माध्यमबाट उपलब्ध गराउन सक्नेछन्। (२) उपदफा (१) को प्रयोजनको लागि नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकेका सार्वजनिक सेवा तोकिएको समयावधि भित्र विद्युतीय माध्यमबाट सम्बन्धित निकायले उपलब्ध गराउनु पर्नेछ। (३) प्रदेश सरकार तथा स्थानीय तहले सार्वजनिक सेवा प्रवाह गर्दा सम्भव भएसम्म विद्युतीय माध्यमको प्रयोग गर्नु पर्नेछ। (४) उपदफा (२) र (३) बमोजिमका सेवा प्रवाह गर्दा विद्युतीय पहिचान (ई-केवाइसी) को व्यवस्था गरी कार्यान्वयनमा ल्याउनु पर्नेछ।
६९.	७०	सूचना विद्युतीय स्वरूपमा राख्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) सरकारी निकाय वा सार्वजनिक संस्थाले आफूले सिर्जना, सङ्कलन तथा प्राप्त गरेका सूचना विद्युतीय स्वरुपमा पनि राख्नु पर्नेछ। (२) उपदफा (१) बमोजिमको सूचना विद्युतीय स्वरुपमा राख्दा सुरक्षा तथा गोपनीयता सम्बन्धी मापदण्ड पूरा गर्नु पर्नेछ। (३) उपदफा (१) बमोजिमको सूचना पुनःप्रयोग गर्न मिल्ने गरी समयबद्ध रुपमा अभिलेखीकरण गर्नु पर्नेछ।
७०.	७१	विद्युतीय माध्यमबाट कारोबार गर्न र अभिलेख राख्न सक्नेः	यस दफामा सरकारी निकाय वा सार्वजनिक संस्था वा नेपालभित्र कारोबार गर्ने बैङ्क वा वित्तीय संस्थाले प्रचलित कानून बमोजिम राख्नु पर्ने अभिलेख तथा गरिने कारोबार विद्युतीय स्वरुप वा विद्युतीय सञ्चार माध्यमको प्रयोग गरी अभिलेख राख्न वा कारोबार गर्न सक्ने व्यवस्था गरिएको छ।
७१.	७२	सूचना प्रविधि	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः-

		प्रणाली प्रयोग गर्नु पर्ने	(१) सरकारी निकाय तथा सार्वजनिक संस्थाले तोकिएको मापदण्ड बमोजिमको सूचना प्रविधि प्रणालीको प्रयोग गर्नु पर्नेछ। (२) सरकारी निकाय तथा सार्वजनिक संस्थाले सूचना प्रविधि प्रणाली मार्फत खुला मानक (ओपन स्ट्याण्डर्ड) मा सूचना संरक्षण गरी राख्न सक्नेछन्। (३) उपदफा (१) बमोजिम सरकारी निकायले सूचना प्रविधि प्रणालीको प्रयोग गर्दा एक अर्का बिच अन्तरआबद्धता हुने गरी तथ्याङ्क तथा सूचना आदानप्रदान गर्नु पर्नेछ। (४) सरकारी निकायले सूचना प्रविधि प्रणाली सञ्चालन गर्नु पूर्व उपदफा (१) बमोजिमको मापदण्ड अनुरुप भए नभएको परीक्षण तोकिएको निकायबाट गराउनु पर्नेछ।
७२.	७३	डिजिटल हस्ताक्षर प्रयोग गर्न सक्ने	यस दफामा सरकारी निकाय र सार्वजनिक संस्थाले आफ्नो कार्य सम्पादन वा सेवा प्रवाह गर्दा यस ऐन बमोजिमको डिजिटल हस्ताक्षर प्रयोग गर्न सक्नेछन् भन्ने व्यवस्था गरिएको छ ।
७३.	७४	वेबसाइट सञ्चालनमा ल्याउनु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) प्रत्येक सरकारी निकाय र सार्वजनिक संस्थाले सूचना तथा सेवा प्रवाह गर्न आफ्नो वेबसाइटको विकास र सञ्चालन गर्नु पर्नेछ। (२) उपदफा (१) बमोजिम सञ्चालन हुने वेबसाइटको विकास र सुरक्षित सञ्चालन सम्बन्धी न्यूनतम मापदण्ड तथा सञ्चालन विधि मन्त्रालयले तोके बमोजिम हुनेछ।
७४.	७५	सूचना प्रविधि प्रणालीको स्वामित्व हस्तान्तरण गर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) दफा ७२ बमोजिमको सूचना प्रविधि प्रणाली वा दफा ७४ बमोजिमको वेबसाइट निर्माणकर्ताले त्यस्तो सूचना प्रविधि प्रणाली वा वेबसाइटसँग सम्बन्धित सोर्स कोड, टेक्निकल डकुमेन्टेसन तथा क्रिडेन्सियल (युजर नेम र पासवर्ड) सहितको सम्पूर्ण संरचना त्यस्तो सूचना प्रविधि प्रणाली वा वेबसाइट सञ्चालन गर्ने सार्वजनिक निकायलाई हस्तान्तरण गर्नु पर्नेछ। (२) यो ऐन प्रारम्भ हुँदाका बखत सञ्चालनमा रहेका सरकारी निकायको सूचना प्रविधि प्रणाली वा वेबसाइटको सोर्स कोड, टेक्निकल डकुमेन्टेसन तथा क्रिडेन्सियल (युजर नेम र पासवर्ड) सहितको सम्पूर्ण संरचनाहरु सार्वजनिक निकायसँग निर्माण तथा सञ्चालन सम्झौता गरिएको भए सो सम्झौतामा

			उल्लिखित अवधिभित्र र त्यस्तो सम्झौता नभएमा यो ऐन प्रारम्भ भएको मितिले तीन महिनाभित्र हस्तान्तरण गर्नु पर्नेछ। (३) उपदफा (१) वा (२) बमोजिम सूचना प्रविधि प्रणाली वा वेबसाइटको सोर्स कोड, टेक्निकल डकुमेन्टेसन तथा क्रिडेन्सियल (युजर नेम र पासवर्ड) सहितको सम्पूर्ण संरचनाहरु हस्तान्तरण नगर्ने निर्माणकर्तालाई विभागले पाँचलाख रुपैयाँसम्म जरिबाना गर्न सक्नेछ।
७५.	७६	सूचना प्रविधि सम्बन्धी प्राविधिक परीक्षण	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) नेपाल सरकारले सरकारी निकायमा प्रयोगमा रहेका सूचना प्रविधि प्रणाली, पूर्वाधार तथा कार्यप्रणालीको आन्तरिक प्राविधिक परीक्षण गर्नका लागि मन्त्रालय अन्तर्गतको कुनै निकायलाई तोक्न सक्नेछ । (२) उपदफा (१) बमोजिमको तोकिएको निकायले देहाय बमोजिम हुने गरी परीक्षण गर्ने गराउनेछः- (क) नेपाल सरकारका संवेदनशील सूचना प्रविधि प्रणाली र पूर्वाधारको कम्तीमा वर्षमा एक पटक प्राविधिक परीक्षण गर्ने गराउने, (ख) सरकारी निकायको अनुरोधको आधारमा सूचना प्रविधि प्रणाली र पूर्वाधारको प्राविधिक परीक्षण गर्ने गराउने, (३) उपदफा (२) बमोजिम परीक्षण सम्पन्न भएपछि परीक्षण गर्ने निकायले सूचना प्रविधि प्रणाली र पूर्वाधारको पूर्णता, दोहोरोपना, सुरक्षा स्थितिको सम्बन्धमा सुझाव सहितको प्रतिवेदन सम्बन्धित निकायलाई उपलब्ध गराउनु पर्नेछ।
७६.	७७	जानकारी दिनु पर्ने	यस दफामा सूचना प्रविधि सम्बन्धी उद्योग स्थापना भएपछि सोको जानकारी विभागलाई दिनु पर्नेछ भन्ने व्यवस्था गरिएको छ।
७७.	७८	स्वीकृत मापदण्डका उपकरण मात्र पैठारी तथा बिक्री वितरण गर्नु पर्ने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) सूचना प्रविधि सम्बन्धी तोकिए बमोजिमका उपकरणको हकमा स्वीकृत मापदण्डको आधारमा मात्र पैठारी तथा बिक्री वितरण गर्न पाइनेछ। (२) उपदफा (१) बमोजिमको मापदण्ड, उपकरणको गुणस्तर, आयु र सुरक्षाको आधारमा स्वीकृत गर्ने प्रक्रिया सम्बन्धी अन्य व्यवस्था तोकिए बमोजिम हुनेछ।
७८.	७९	नवीनतम प्रविधिको प्रयोग	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः-

			(१) सूचना प्रविधिको क्षेत्रमा विकसित भएका नवीनतम प्रविधिको पारदर्शी, जवाफदेही, सुरक्षित र मर्यादित प्रयोग गर्नु पर्नेछ। स्पष्टीकरणः यस दफाको प्रयोजनको लागि "नवीनतम प्रविधि" भन्नाले सूचना प्रविधिको क्षेत्रमा नयाँ र द्रुत गतिमा विकसित भएका कृत्रिम बौद्धिकता, मेसिन लर्निङ्ग, वल्कचेन, ईन्टरनेट अफ थिङ्गस, फाइभ जी तथा नेक्सट जेनरेसन नेटवर्क, क्वान्टम कम्प्युटिङ्ग लगायतका प्रविधि सम्झनु पर्छ। (२) उपदफा (१) बमोजिमको नवीनतम् प्रविधिको उपयोग, प्रवर्धन र विस्तार सरकारी, सार्वजनिक र निजी क्षेत्रको सहकार्यमा गर्न सकिनेछ। (३) उपदफा (१) बमोजिमको नवीनतम प्रविधिको व्यवस्थित प्रयोगको लागि विभागले समन्वय र सहजीकरण गर्नेछ।
७९.	८०	मुलुकको साइबर सुरक्षा तथा तथ्याङ्क प्रणालीमा अवरोध सिर्जना गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले विद्युतीय प्रणालीको प्रयोग गरी मुलुकको साइबर सुरक्षा तथा तथ्याङ्क प्रणालीमा अवरोध सिर्जना गर्ने वा प्रतिकूल असर पार्ने कुनै कार्य गर्न वा गराउन हुदैन। (२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी पाँच वर्षसम्म कैद वा दशलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।
८०.	८१	विद्युतीय प्रणालीको कार्य सञ्चालनमा हस्तक्षेप गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले आफू वा अरु कसैलाई आर्थिक वा अन्य लाभ पुऱ्याउने नियतले अनधिकृत रुपमा विद्युतीय सूचना प्रविष्ट वा सम्प्रेषण वा हेरफेर गरी वा मेटाई वा लुकाई छिपाई विद्युतीय प्रणालीको कार्य सञ्चालनमा हस्तक्षेप गर्न वा कसैलाई आर्थिक नोक्सानी हुने गरी निजको संवेदनशील वित्तीय सूचना प्राप्त गर्न वा गराउन हुँदैन। (२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी तीन वर्षसम्म कैद वा पाँचलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
८१.	८२	विद्युतीय प्रणालीको स्रोत सङ्केत नष्ट, परिवर्तन गर्न वा चोरी गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले विद्युतीय प्रणालीमा प्रयोग हुने स्रोत सङ्केत तथा सूचनाको चोरी गर्न, अनधिकृत रुपमा नष्ट गर्न वा परिवर्तन गर्न हुँदैन। स्पष्टीकरण: यस दफाको प्रयोजनका लागि "स्रोत सङ्केत" भन्नाले कम्प्युटर कार्यक्रमको सूचीकरण, कम्प्युटर निर्देशन, कम्प्युटर डिजाइन र कम्प्युटर

			लेआउट तथा कम्प्युटर सम्पदाको जुनसुकै स्वरुपमा रहेको कार्यक्रम विश्लेषण सम्झनु पर्छ। (२) कसैले विद्युतीय प्रणालीमा प्रयोग हुने स्रोत सङ्केत तथा सूचना चोरीको हो भन्ने जानी जानी खरिद तथा बिक्री गर्न हुँदैन। (३) उपदफा (१) वा (२) बमोजिमको कसूर गरेमा कसूरको मात्र हेरी तीन वर्षसम्म कैद वा पाँचलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।
८२.	८३	कम्प्युटर प्रणालीमा अनधिकृत पहुँच पुऱ्याउन, सूचना प्रविष्ट गर्न, हेरफेर गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीमा अनधिकृत पहुँच पुऱ्याउन वा त्यस्तो प्रणालीमा प्रवेश गरी डाटाको अखण्डतामा फरक पर्ने गरी डाटा हेरफेर गर्ने वा मेटाउने कार्य गर्नु वा गराउनु हुँदैन। (२) 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 हुँदैन। (३) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुई लाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
८३.	८४	विद्युतीय प्रणालीमा अवरोध गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले कुनै विद्युतीय प्रणालीको कार्य सञ्चालनमा बाधा पुऱ्याउन वा प्रयोगकर्तालाई प्रणाली प्रयोगमा अबरोध गर्न, रोक लगाउन वा हस्तक्षेप गर्न हुँदैन। (२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी तीन वर्षसम्म कैद वा तीनलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।
८४.	८५	विद्युतीय स्वरुपको सूचनालाई क्षति पुऱ्याउन, अवरोध गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले गलत मनसाय राखी कसैको स्वामित्व वा नियन्त्रणमा रहेको विद्युतीय स्वरुपको सूचनालाई अनधिकृत रुपमा मेटाउन, नष्ट गर्न, हेरफेर गर्न, बिगार्न, बुझ्न नसकिने गरी परिवर्तन गर्न वा अर्थहीन, प्रयोगहीन वा निष्प्रभावी गराउन वा सूचनाको प्रयोगलाई अनधिकृत रुपमा बाधा पुऱ्याउन, रोक लगाउन वा आधिकारिक व्यक्तिलाई सूचनामा पहुँच दिन ईन्कार गर्न हुँदैन।

			(२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्र हेरी तीन वर्षसम्म कैद वा तीनलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
८५.	८६	गोपनीयता भङ्ग गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले यस ऐन विपरीत विद्युतीय माध्यमबाट कसैको वैयक्तिक विवरण संकलन गरेमा वा सूचना, जानकारी अनधिकृत रूपमा प्राप्त गर्न, त्यसको गोपनीयता भङ्ग गर्न वा अनधिकृत रूपमा कसैलाई उपलब्ध गराउन हुँदैन। (२) कसैले पनि कुनै दुई वा दुईभन्दा बढी व्यक्तिबिचमा विद्युतीय माध्यमबाट भएका कुनै वैयक्तिक संवाद वा कुराकानी वा सङ्केत सम्बन्धित व्यक्तिले 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, (क) सार्वजनिक रूपमा गरिएको भाषण वा वक्तव्यको हकमा यस उपदफाको व्यवस्था लागू हुने छैन। (ख) प्रचलित कानून बमोजिमको अवस्थामा कुनै पनि सूचना वा जानकारीको ध्वनि अङ्कन वा रेकर्ड गर्न वा गराउन सकिनेछ। (३) उपदफा (१) वा (२) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा तीनलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।
८६.	८७	झुट्टा प्रमाणपत्र प्रकाशन गर्न वा उपलब्ध गर्न, गराउन नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले प्रमाणीकरण निकायले प्रमाणपत्र जारी गरेको होइन वा सो प्रमाणपत्रमा सूचीकृत गरिएको ग्राहकले स्वीकार गरेको छैन वा सो प्रमाणपत्र निलम्बन वा रद्द भइसकेको छ भन्ने जानीजानी त्यस्तो प्रमाणपत्रको प्रकाशन गर्न वा अन्य कसैलाई कुनै ब्यहोराले उपलब्ध 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 गराइएको विषयमा यस दफा बमोजिम कसूर मानिने छैन। (२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रूपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।

८७.	८८	अश्लील सामग्री उत्पादन, वितरण, प्रकाशन, प्रसार वा खरिद बिक्री गर्न वा गराउन नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले विद्युतीय प्रणालीको माध्यमबाट कुनै अश्लिल सामग्रीको उत्पादन तथा सङ्कलन गर्न, बिक्री वितरण गर्न, प्रकाशन गर्न, प्रदर्शन गर्न, प्रसार गर्न वा सञ्चय गर्न हुँदैन। तर कुनै व्यक्तिले कुनै अनुसन्धान, कानून कार्यान्वयन, अध्यापन वा चिकित्सकीय प्रयोजनको लागि यौनजन्य सामग्रीको सम्प्रेषण, प्राप्ति वा सञ्चय गरेको प्रमाणिक रूपमा देखाउन सकेमा र त्यस्तो उद्देश्य पूरा हुनासाथ त्यस्ता सामग्री मेटाएमा यस दफा बमोजिमको कसूर मानिने छैन। (२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
८८.	८९	गोप्य कोड चोरी गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) 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। स्पष्टीकरणः यस दफाको प्रयोजनको लागि,- (क) "फिसिङ्ग" भन्नाले विद्युतीय सञ्चार माध्यमबाट कुनै कुरा सत्य हो भन्ने विश्वासमा पारी कुनै व्यक्तिको युजरनेम र पासवर्ड,क्रेडिट कार्ड नम्बर, बैङ्क एकाउन्ट जस्ता संवेदनशील सूचना प्राप्त गर्ने कार्य सम्झनु पर्छ र सो शब्दले नक्कली लिङ्क प्रयोग गरी साइबर स्पेसका प्रयोगकर्तालाई झुक्याई संवेदनशील जानकारी प्रवाह गर्न प्रेरित गर्ने वा कुनै मालवेयर स्थापना गर्ने कार्य सम्झनु पर्छ। (ख) "स्पुफिङ" भन्नाले कसैले अज्ञात स्रोतबाट भएको सञ्चारलाई ज्ञात र विश्वसनीय स्रोतबाट आएको भनी झुक्याउने कार्य सम्झनु पर्छ। (२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
८९.	९०	कम्प्युटर प्रणालीबाट डाटा चोरी गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको युजर एकाउन्ट वा कम्प्युटर प्रणालीबाट वा स्निफिङ लगायतका विधि प्रयोग गरी नेटवर्कमा प्रसारित डाटालाई चोरी गर्नु वा गराउनु हुँदैन।

			स्पष्टीकरणः यस दफाको प्रयोजनको लागि "स्निफिङ" भन्नाले कसैले दुई वा सोभन्दा बढी पक्ष बिच भएको डाटा आदानप्रदानमा सम्बन्धित पक्षको अनुमति बिना अनधिकृत रुपमा उक्त डाटा सुन्ने, पढ्ने वा हेर्ने कार्य सम्झनु पर्छ। (२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।
९०.	९१	कम्प्युटर प्रणालीमा अवाञ्छित एप्लिकेशन फैलाउन नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले विद्युतीय माध्यमको प्रयोग गरी कसैको कम्प्युटर वा कम्प्युटर प्रणालीमा अनुमतिबिना अवाञ्छित एप्लिकेशन प्रवेश गराउने वा फैलाउने कार्य गर्नु वा गराउनु हुँदैन। (२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
९१.	९२	सार्वजनिक सूचना प्रणालीमा अवरोध गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले सार्वजनिक प्रयोगमा रहेको कम्प्युटर वा कम्प्युटर प्रणालीको सञ्जाललाई डिनायल अफ सर्भिस लगायतका विधि प्रयोग गरी बन्द गर्ने वा कम्प्युटर प्रणालीको अपेक्षित प्रयोगकर्ताका लागि कम्प्युटर प्रणालीमा पहुँच नपुग्ने वातावरण सिर्जना हुने कार्य गर्नु वा गराउनु हुँदैन। स्पष्टीकरणः यस दफाको प्रयोजनको लागि "डिनायल अफ सर्भिस" भन्नाले कसैले सार्वजनिक रुपमा सेवा प्रदान गर्ने कम्प्युटर प्रणाली बन्द गर्ने वा उक्त प्रणालीबाट प्रदान गरिने सेवा अवरुद्ध हुने गरी आक्रमण गर्ने कार्य सम्झनु पर्छ। (२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।
९२.	९३	इन्टरनेट अफ थिङ्गसमा आक्रमण गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले इन्टरनेट अफ थिङ्गसमा आधारित उपकरण तथा सञ्जालमा अनुमति बिना आक्रमण गरी सो सञ्जालको निर्धारित काममा खलल पुऱ्याउने कार्य गर्नु वा गराउनु हुँदैन। स्पष्टीकरणः यस दफाको प्रयोजनको लागि “इन्टरनेट अफ थिङ्गस” भन्नाले एक अर्का बिच डाटा आदानप्रदान गर्न सक्ने इलेक्ट्रोमेकानिकल उपकरणको सामूहिक सञ्जाल सम्झनु पर्छ।

			(२) उपदफा (१) बमोजिमको कसूर गर्नेलाई कसूरको मात्रा हेरी दुई वर्षसम्म कैद वा दुईलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
९३.	९४	पहिचानको दुरुपयोग गर्न नहुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कसैले विद्युतीय माध्यममा रहेको व्यक्तिको निजी साँचो, पासवर्ड वा अन्य विद्युतीय स्वरुपमा रहेको पहिचानको स्थानान्तरण, नियन्त्रण वा प्रयोग गरी प्रचलित कानून बमोजिम कसूर मानिने कार्य गर्ने मनसायले पहिचानको दुरुपयोग गर्नु हुँदैन। (२) उपदफा (१) बमोजिमको कसूर गरेमा कसूरको मात्रा हेरी एक वर्षसम्म कैद वा एकलाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ।
९४.	९५	कृत्रिम बौद्धिकता (आर्टिफिसियल इन्टेलिजेन्स) को प्रयोग गरी कसूर गरेमा सजाय हुने	यस दफामा कसैले यस ऐन बमोजिम कसूर मानिने कार्य कृत्रिम बौद्धिकता (आर्टिफिसियल इन्टेलिजेन्स) को प्रयोग गरी गरेमा त्यस्तो कसूर सोही व्यक्तिले गरे सरह मानी सजाय हुने व्यवस्था गरिएको छ।
९५.	९६	कसूर गर्न दुरुत्साहन गर्न नहुने	यस दफामा कसैले यस ऐन बमोजिमको कुनै कसूर गर्न दुरुत्साहन गरेमा वा अपराधिक षडयन्त्रमा संलग्न भएमा त्यस्तो व्यक्तिलाई मुख्य कसूरदारलाई भए सरहको सजाय हुने व्यवस्था गरिएको छ।
९६.	९७	मतियारलाई हुने सजायः	यस दफामा यस ऐन बमोजिमको कुनै कसूर गर्न सघाउने वा अन्य कुनै ब्यहोराले मतियार भई कार्य गर्ने व्यक्तिलाई मुख्य कसूरदारलाई भएको सजायको आधा सजाय हुने व्यवस्था गरिएको छ।
९७.	९८	सङ्गठित संस्थाबाट भएको कसूरः	यस दफामा कुनै फर्म वा कम्पनी वा सङ्गठित संस्थाले यस ऐन बमोजिमको कसूर मानिने कुनै काम गरे वा गराएमा त्यस्तो कार्य गर्ने गराउने व्यक्ति जिम्मेवार हुनेछ र त्यस्तो व्यक्ति किटान हुन नसकेमा फर्म, कम्पनी वा सङ्गठित संस्थाको हकमा कार्यकारी प्रमुख भई काम गर्ने सम्बन्धित धनी वा हिस्सेदार, सञ्चालक, प्रबन्ध सञ्चालक वा महाप्रबन्धकले आपराधिक दायित्व ब्यहोर्नु पर्ने व्यवस्था गरिएको छ।
९८.	९९	प्रचलित कानून बमोजिम सजाय गर्न बाधा नपर्नेः	यस दफामा 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 भन्ने व्यवस्था गरिएको

			छ।
९९.	१००	क्षतिपूर्ति भराउनु पर्ने	यस दफामा यस ऐन बमोजिम कसूर गरेको कारणबाट कसैलाई कुनै किसिमको हानी, नोक्सानी, हैरानी वा क्षति भएको रहेछ भने त्यस्तो हानी, नोक्सानी, हैरानी वा क्षतिको क्षतिपूर्ति सम्बन्धित कसूरदारबाट भराई दिनु पर्ने व्यवस्था गरिएको छ।
१००	१०१	नेपाल सरकार वादी हुने	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (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।
१०१	१०२	हदम्याद	यस दफामा यो ऐन बमोजिमको कसूर भए गरेको थाहा पाएको मितिले छ महिना भित्र उजुर गर्नु पर्ने व्यवस्था गरिएको छ।
१०२	१०३	पुनरावेदन	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- ऐनको दफा १६ को उपदफा (५) र दफा २० को उपदफा (६) बमोजिम नियन्त्रकले गरेको जरिवाना, दफा ४२ को उपदफा (२), दफा ४५ को उपदफा (२) र दफा ७५ को उपदफा (३) बमोजिम विभागले गरेको जरिवाना र दफा ४८ को उपदफा (२) र दफा ५९ को उपदफा (६) बमोजिम केन्द्रले गरेको जरिवाना उपर चित्त नबुझेमा त्यस्तो निर्णय भएको थाहा पाएको मितिले पैंतिस दिनभित्र जिल्ला अदालतमा पुनरावेदन गर्न सकिनेछ।
१०३	१०४	अनुसन्धान अधिकृत	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) यस ऐन बमोजिमको कसूर सम्बन्धी मुद्दाको अनुसन्धान सूचना प्रविधि सम्बन्धी ज्ञान भएको कम्तीमा प्रहरी निरीक्षकस्तरको अधिकृतले गर्नेछ। (२) उपदफा (१) बमोजिम अनुसन्धान गर्दा अनुसन्धान अधिकृतले प्राविधिक विषयमा विभागसँग समन्वय गर्न सक्नेछ।
१०४	१०५	द्रुत संरक्षण	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कुनै विद्युतीय उपकरणमा भण्डारण गरिएको सूचना कुनै फौजदारी कसूरको अनुसन्धानको लागि आवश्यक रहेको र त्यस्तो सूचना नष्ट हुन सक्ने वा पहुँचबाट हटाईन सक्ने सम्भावना रहेको कुरामा अनुसन्धान अधिकृत विश्वस्त भएमा त्यस्तो विद्युतीय उपकरण वा सूचना नियन्त्रणमा रहेको व्यक्तिलाई अनुसन्धान अधिकृतले लिखित सूचना दिई बढीमा सात दिनसम्म 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 अनुसन्धान अधिकृतको आदेशको पालना गर्नु सम्बन्धित व्यक्तिको कर्तव्य हुनेछ।
१०५	१०६	ट्राफिक तथ्याङ्कमा पहुँच पुऱ्याउन सक्ने	यस दफामा कुनै खास सञ्चारसँग सम्बद्ध ट्राफिक तथ्याङ्क कुनै कसूरको अनुसन्धान प्रयोजनको लागि अदालतले तत्काल प्राप्त प्रमाणको आधारमा आवश्यक ठानेमा अनुसन्धान अधिकृतलाई खास सञ्चार सम्बन्धी ट्राफिक तथ्याङ्कमा पहुँच राख्न अनुमति दिन सक्ने व्यवस्था गरिएको छ।
१०६	१०७	ट्राफिक तथ्याङ्कको सङ्कलन	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) कुनै खास सञ्चारसँग सम्बन्धित ट्राफिक तथ्याङ्क कुनै कसूरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक देखेमा उक्त ट्राफिक तथ्याङ्कमा नियन्त्रण गर्न देहाय बमोजिमको आदेश गर्न सक्नेछः- (क) तोकिएको अवधिमा खास सञ्चारसँग सम्बद्ध ट्राफिक तथ्याङ्कको सञ्चार हुँदाहुँदैको अवस्था (रियल टाइम)मा सङ्कलन वा अभिलेखन गर्न, वा (ख) सम्बद्ध ट्राफिक तथ्याङ्कको सञ्चार हुँदाहुँदैको अवस्थामा सङ्कलन वा अभिलेखन गर्न अनुसन्धान अधिकृतलाई अनुमति प्रदान गर्न वा सहयोग गर्न। (२) कुनै खास सञ्चारसँग 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 सङ्कलन वा अभिलेखन गर्न अनुमति प्रदान गर्न सक्नेछ।
१०७	१०८	विषयवस्तुको अन्तरदोहन (इन्टरसेप्सन)	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) सञ्चारको कुनै विषयवस्तु कसूरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक देखेमा सेवा प्रदायकलाई प्रविधिको प्रयोग गरी विद्युतीय प्रणाली मार्फत प्रसार भएको खास सञ्चारको विषयवस्तु प्रसार हुँदाहुँदैको अवस्थामा सङ्कलन 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 देखेमा सञ्चारको विषयवस्तु प्रसार हुँदाहुँदैको अवस्थामा सङ्कलन वा अभिलेख गर्न अनुसन्धान अधिकृतलाई अख्तियारी प्रदान गर्न सक्नेछ।
१०८	१०९	विद्युतीय प्रमाणको ग्राह्यताः	यस दफामा कुनै कसूर विरुद्धको कारबाहीको क्रममा प्रचलित कानून बमोजिम विद्युतीय प्रणालीबाट सिर्जना भएको विद्युतीय वा अन्य कुनै स्वरुपमा रहेको कुनै सूचना वा तथ्याङ्क प्रमाणको रुपमा ग्राह्य हुने व्यवस्था गरिएको छ।
१०९	११०	अनुसन्धान तथा तालिम केन्द्र स्थापना र सञ्चालनः	यस दफामा नेपाल सरकारले सूचना प्रविधि तथा साइबर सुरक्षाको सम्बन्धमा अध्ययन, अनुसन्धान तथा विकास गर्न र सो सम्बन्धी विषयमा तालिम सञ्चालन गर्न अनुसन्धान तथा तालिम केन्द्रको स्थापना र सञ्चालन गर्न सक्ने व्यवस्था गरिएको छ।
११०	१११	नियम बनाउने अधिकारः	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) यस ऐनको उद्देश्य कार्यान्वयन गर्न नेपाल सरकारले आवश्यक नियम बनाउन सक्नेछ। (२) उपदफा (१) ले दिएको अधिकारको सर्वसामान्यतामा प्रतिकूल प्रभाव नपर्ने गरी देहायको विषयमा नियम बनाउन सकिनेछः- (क) सुरक्षित विद्युतीय अभिलेख तथा परीक्षण विधि, (ख) विद्युतीय अभिलेखको प्राप्ति,स्वीकार तथा सोको जानकारी, (ग) डिजिटल हस्ताक्षर, डिजिटल हस्ताक्षरको सुरक्षण कार्यविधि तथा परीक्षण र सम्पुष्टि, (घ) नियन्त्रक तथा प्रमाणीकरण निकायको काम, कर्तव्य र अधिकार, (ङ) प्रमाणीकरण निकायको योग्यता, इजाजतपत्र र सोको दस्तुर, इजाजतपत्रको निलम्बन तथा रद्द गर्ने तथा नवीकरण र सेवा शुल्क, (च) विदेशी प्रमाणीकरण निकायलाई मान्यता दिँदा अपनाउनु पर्ने कार्यविधि, (छ) डिजिटल हस्ताक्षर सम्बन्धी प्रमाणपत्र, प्रमाणपत्रको निलम्बन, फुकुवा वा रद्द, (ज) कार्यसम्पादन परीक्षकको योग्यता, नियुक्ति, सेवा अवधि, पारिश्रमिक र परीक्षण,

			(झ) विद्युतीय माध्यमबाट प्रदान गरिने सरकारी सेवा, सेवा प्राप्त गर्ने प्रक्रिया, (ञ) प्रयोगकर्ताले जोडी साँचो सिर्जना गर्दा अपनाउनु पर्ने प्रक्रिया, (ट) विद्युतीय माध्यमबाट गरिने कारोबारको अभिलेख तथा भुक्तानी, (ठ) डोमेन नाम दर्ता, नवीकरण तथा दस्तुर, एनपी डोमेन नाम सञ्चालन, (ड) सूचना प्रविधि सम्बन्धी उद्योग र व्यवसाय सञ्चालनको स्वीकृति, नवीकरण र खारेज, (ढ) सूचना प्रविधि सम्बन्धी उपकरणको पैठारी तथा बिक्री वितरण, (ण) नवीनतम प्रविधिको प्रयोग, (त) सरकारी तथा सार्वजनिक निकायमा प्रयोग भएको सूचना प्रविधिको सुरक्षाको परीक्षण, (थ) डाटा सेन्टर वा क्लाउडको इजाजतपत्र, सोको नवीकरण शुल्क तथा दस्तुर, (द) साइबर सुरक्षा प्रदायक सूचीकृत सम्बन्धी, (ध) संवेदनशील सूचना पूर्वाधार, र (न) अनुसन्धान तथा तालिम केन्द्रको स्थापना र सञ्चालन।
१११	११२	मापदण्ड बनाउने	यस दफामा यो ऐन कार्यान्वयन गर्न मन्त्रालयले देहायको विषयमा मापदण्ड बनाउन सक्ने व्यवस्था गरिएको छः- (क) विद्युतीय सूचना तथा डिजिटल हस्ताक्षरको गोपनीयता र सुरक्षा, (ख) सरकारी निकायमा कम्प्युटर तथा सूचना प्रविधि प्रणालीको प्रयोग, (ग) सरकारी निकाय तथा सार्वजनिक संस्थाको वेबसाइट, (घ) सूचना प्रविधि प्रणाली र पूर्वाधारको प्राविधिक परीक्षण, (ङ) डाटा सेन्टर वा क्लाउड सेवा मापदण्ड, र (च) साइबर सुरक्षाको मापदण्ड।
११२	११३	खारेजी र बचाउ	यस दफामा देहाय बमोजिम व्यवस्था गरिएको छः- (१) विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ खारेज गरिएको छ। (२) विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ बमोजिम भए गरेका काम कारबाही यसै ऐन बमोजिम भए गरेको मानिनेछ।