Cybersecurity

www.shutterstock.com · 1187828911

साईबर सुरक्षा गर्ने सम्बन्धमा व्यवस्था गर्न बनेको विधेयक

प्रस्तावना: साईबर सुरक्षा खतरा तथा साईबर सुरक्षाका घटना रोकथाम गर्न, साईबर सुरक्षाका घटना सम्बन्धी प्रतिक्रियात्मक कार्य गर्न तथा अनुसन्धान गर्न, संवेदनशील सूचना पूर्वाधारका धनी तथा साईबर सुरक्षा सेवा प्रदायकलाई नियमन तथा व्यवस्थित गर्न वाञ्छनीय भएकोले,

संघीय संसदले यो ऐन बनाएको छ ।

परिच्छेद- १

प्रारम्भिक

१. **संक्षिप्त नाम, विस्तार र प्रारम्भ**: (१) यस ऐनको नाम "साईबर सुरक्षा ऐन, २०७९" रहेको छ ।

(२) यो ऐन नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकेको मिति देखि प्रारम्भ हुनेछ ।

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

(क) "अडिटर" भन्नाले कुनै कम्प्युटर वा कम्प्युटर प्रणालीको साईवर सुरक्षा कमजोरी निर्धारण, परीक्षण वा मूल्याङ्कन गर्न दफा २८ बमोजिम अनुमतिपत्र प्राप्त गरेको व्यक्तिलाई सम्झनु पर्छ ।

(ख) "अत्यावश्यक सेवा" भन्नाले नेपालको राष्ट्रिय सुरक्षा, प्रतिरक्षा, वैदेशिक सम्बन्ध, अर्थतन्त्र, सार्वजनिक स्वास्थ्य, सार्वजनिक सुरक्षा वा शान्ति र व्यवस्था तथा अनुसूची- १ मा समावेश गरिएका कुरालाई सम्झनु पर्छ ।

(ग) "अनुमतिपत्र" भन्नाले दफा २८ बमोजिम प्रदान गरिने साईबर सुरक्षा सेवा प्रदायक अनुमतिपत्र सम्झनु पर्छ ।

(घ) "अनुमतिपत्रयोग्य साईबर सुरक्षा सेवा" भन्नाले अनुसूची- २ मा तोकिएका अनुमतिपत्रयोग्य साईबर सुरक्षा सेवा सम्झनु पर्छ ।

(ङ) "अनुमतिपत्रवाहक" भन्नाले अनुमतिपत्र प्राप्त व्यक्तिलाई सम्झनु पर्छ ।

(च) "कम्प्युटर" भन्नाले विद्युतीय, चुम्बकीय, अप्टिकल, ईलेक्ट्रो केमिकल वा लोजिकल, अर्थमेटिक जस्ता तथ्याङ्क प्रशोधन गर्ने वा भण्डारण गर्ने कार्य गर्ने उपकरण सम्झनु पर्छ र सो शब्दले प्रत्यक्ष रुपमा यस्ता उपकरण सँगको संयोजनमा संचालनमा आउने कुनै तथ्याङ्क भण्डारण सुविधा वा संचार सुविधा समेतलाई जनाउँछ ।

(छ) "कम्प्युटर प्रोग्राम" भन्नाले तथ्याङ्क प्रतिनिधित्व गर्ने निर्देशन वा कम्प्युटरमा प्रयोग गरिएमा कार्य सम्पादन गर्न सक्ने जुनसुकै कथन सम्झनु पर्छ ।

(ज) "कम्प्युटर प्रणाली" भन्नाले आगत र निर्गत (इन्पुट र आउटपुट) सहायता संयन्त्र लगायतका कम्प्युटर कार्यक्रम, विद्युतीय निर्देशन, आगत र निर्गतका तथ्याङ्कहरु समाविष्ट भएको र तार्किक, अङ्कगणीतीय, तथ्याङ्क सञ्चय तथा पुनः प्राप्ति, संचार र नियन्त्रण लगायतका कार्यहरु सम्पादन गर्ने संयन्त्र वा संयन्त्रहरुको संजाल सम्झनु पर्छ ।

(झ) "कम्प्युटर सेवा" भन्नाले कम्प्युटर समय, तथ्याङ्क प्रशोधन तथा भण्डारण वा तथ्याङ्कको पुनः प्राप्ति सम्झनु पर्छ ।

(ञ) "केन्द्र" भन्नाले दफा ३ बमोजिम गठन भएको राष्ट्रिय साईबर सुरक्षा केन्द्र सम्झनु पर्छ ।

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

(ठ) "प्रमुख कार्यकारी अधिकृत" भन्नाले दफा ३९ बमोजिम नियुक्त प्रमुख कार्यकारी सम्झनु पर्छ ।

(ड) "मन्त्रालय" भन्नाले सञ्चार तथा सूचना प्रविधि मन्त्रालय सम्झनु पर्छ ।

(ढ) "समिति" भन्नाले दफा ६ बमोजिमको समिति सम्झनु पर्छ ।

(ण) "साईबर सुरक्षा" भन्नाले कम्प्युटर वा कम्प्युटर प्रणालीलाई अनाधिकृत पहुँच वा आक्रमणबाट सुरक्षित राख्न सकिने अवस्थालाई सम्झनु पर्छ र जसको कारणले-

(१) कम्प्युटर वा कम्प्युटर प्रणाली निरन्तर रुपमा उपलब्ध र संचालनमा रहनेछ,

(२) कम्प्युटर वा कम्प्युटर प्रणाली सुरक्षित रहनेछ,

(३) कम्प्युटर वा कम्प्युटर प्रणालीमा भण्डारण गरिएको सूचनाको गोपनियता, प्रशोधन गरिएको वा प्रशारण गरिएका कुरा सुरक्षित रहनेछन् ।

(त) "साईबर सुरक्षा अधिकृत" भन्नाले दफा २२ बमोजिम तोकिएको साईबर सुरक्षा अधिकृत सम्झनु पर्छ ।

(थ) "साईबर सुरक्षा खतरा" भन्नाले कानून बमोजिम अधिकार प्राप्त नगरी कम्प्युटर वा कम्प्युर प्रणाली मार्फत अर्को कुनै कम्प्युटर प्रणालीको साईबर सुरक्षामा नकारात्मक प्रभाव पार्ने गरी गरिएको कुनै पनि क्रियाकलाप सम्झनु पर्छ ।

(द) "साईबर सुरक्षा घटना" भन्नाले कानून बमोजिम अख्तियार प्राप्त नगरी कम्प्युटर वा कम्प्युर प्रणाली मार्फत अर्को कम्प्युटर वा कम्प्युर प्रणालीको साईबर सुरक्षा खतरामा पार्ने वा नकारात्मक प्रभाव पार्ने गरी गरिएको क्रियाकलाप सम्झनु पर्छ ।

(ध) "साईबर सुरक्षा प्रोग्राम" भन्नाले कम्प्युटर वा कम्प्युटर प्रणालीको साईबर सुरक्षा सुनिश्चित गर्न वा सुदृढ पार्न डिजाईन गरिएको कम्प्युटर प्रोग्राम सम्झनु पर्छ ।

(न) "साईबर सुरक्षा सेवा" भन्नाले कुनै व्यक्तिले शुल्क लिएर अर्को कुनै व्यक्तिको कम्प्युटर वा कम्प्युटर प्रणालीको साईबर सुरक्षा सुनिश्चित गर्न वा सुदृढ बनाउन प्रदान गर्ने सेवालाई सम्झनु पर्छ र यो शब्दले देहायका कुरा समेत समावेश गर्नेछ:-

(१) कुनै व्यक्तिको कम्प्युटर वा कम्प्युटर प्रणालीको साईबर सुरक्षा प्रतिरक्षा कमजोरीहरु पत्ता लगाई कम्प्युटर वा कम्प्युटर प्रणालीको साईबर सुरक्षाको समिक्षा गर्ने, परीक्षण गर्ने वा मूल्याङ्कन गर्ने,

(२) कुनै व्यक्तिको कम्प्युटर वा कम्प्युटर प्रणालीको फोरेन्सिक परीक्षण संचालन गर्ने,

(३) कुनै व्यक्तिको कम्प्युटर वा कम्प्युटर प्रणालीमा भएको साईबर सुरक्षा घटना छानविन गर्ने तथा समाधान गर्ने,

(४) साईबर सुरक्षा खतरा वा घटना पत्ता लगाउन कुनै व्यक्तिको कम्प्युटर वा कम्प्युटर प्रणालीको सम्पूर्ण परीक्षण संचालन गर्ने,

(५) एक वा एक भन्दा बढी साईबर सुरक्षा उपायको डिजाईन गर्ने, बिक्री गर्ने, आयात गर्ने, निर्यात गर्ने, जडान गर्ने, बचाउने, वा मरम्मत गर्ने,

(६) कम्प्युटर वा कम्प्युटर प्रणालीको साईबर सुरक्षा खतरा पहिचान गर्ने प्रयोजनको लागि कुनै व्यक्तिको कम्प्युटर वा कम्प्युटर प्रणालीमा भण्डारण गरिएको, प्रशोधन गरिएको वा प्रशारण गरिएको कुरा प्राप्त, पहिचान वा स्क्यान गरी साईबर सुरक्षाको अनुगमन गर्ने,

(७) साईबर सुरक्षा प्रोग्राम वा साईबर सुरक्षा खतरा पत्ता लगाउने वा समिक्षा गर्ने, समाधानका उपाय वा साईबर सुरक्षा जोखिम कम गर्न व्यवस्थापन रणनीति सम्बन्धमा परामर्श दिने,

(८) सम्बन्धित संस्थाको साईबर सुरक्षा नीतिको पालना भए नभएको समिक्षा वा अनुगमन गर्ने,

(९) साईबर सुरक्षा प्रोग्राम वा साईबर सुरक्षा खतरा पत्ता लगाउने वा समिक्षा गर्ने, समाधानका उपाय वा साईबर सुरक्षा खतरा कम गर्न व्यवस्थापन रणनीति सम्बन्धमा परामर्श दिने,

(१०) साईबर सुरक्षा सुदृढ बनाउने कुनै पनि प्रचलनका बारेमा राय परामर्श प्रदान गर्ने,

(११) साईबर सुरक्षा सेवा सम्बन्धी तालीम वा शिक्षा दिने ।

(प) "साईबर सुरक्षा सेवा प्रदायक" भन्नाले साईबर सुरक्षा सेवा प्रदान गर्ने व्यक्तिलाई सम्झनु पर्छ ।

(फ) "साईबर सुरक्षा सोलुसन" भन्नाले अर्को कुनै कम्प्युटर वा कम्प्युटर प्रणालीको साईवर सुरक्षा सुनिश्चित गर्न वा सुदृढ पार्न, डिजाईन गरिएको कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर प्रोग्राम वा डिजाईन गरिएको कम्प्युटर सेवा सम्झनु पर्छ ।

(ब) "संवेदनशील सूचना पूर्वाधार" भन्नाले अनुसूची- १ मा समावेश गरिएका अत्यावश्यककम्प्युटर वा कम्प्युटर प्रणाली सम्झनु पर्छ ।

(भ) "संवेदनशील सूचना पूर्वाधारको धनी" भन्नाले संवेदनशील सूचना पूर्वाधारको धनी सम्झनु पर्छ र त्यस्तो संवेदनशील सूचना पूर्वाधारको धनी एक भन्दा बढी भएमा प्रत्येक शेयरधनी समेतलाई जनाउनेछ ।

परिच्छेद- २

राष्ट्रिय साईबर सुरक्षा केन्द्रको स्थापना, काम, कर्तव्य र अधिकार

३. **राष्ट्रिय साईबर सुरक्षा केन्द्रको स्थापनाः** (१) देशभित्र रहेका कम्प्युटर वा कम्प्युटर प्रणालीलाई साईबर सुरक्षा प्रदान गर्न सोसँग सम्बन्धित अन्य कार्य गर्न राष्ट्रिय साईबर सुरक्षा केन्द्रको स्थापना गरिएको छ ।

(२) केन्द्रको कार्यालय काठमाडौं उपत्यकामा रहनेछ ।

४. **केन्द्र स्वशासित संस्था हुनेः** (१) केन्द्र अविच्छिन्न उत्तराधिकारवाला स्वशासित संगठित संस्था हुनेछ ।

(२) केन्द्रको काम कारबाहीको लागि एउटा छुट्टै छाप हुनेछ ।

(३) केन्द्रले व्यक्ति सरह चल अचल सम्पत्ति प्राप्त गर्न, उपभोग गर्न बेचविखन गर्न वा अन्य कुनै किशिमले व्यवस्था गर्न सक्नेछ ।

(४) केन्द्रले व्यक्ति सरह आफ्नो नामबाट नालिस उजुर गर्न र केन्द्र उपर पनि सोही नामले नालिस उजुर लाग्न सक्नेछ ।

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

(क) साईबर सुरक्षा बारेमा नीति निर्माण गर्न नेपाल सरकारलाई परामर्श दिने,

(ख) कम्प्युटर र कम्प्युटर प्रणालीको साईबर सुरक्षा निरीक्षण गर्ने गर्ने,

(ग) साईबर सुरक्षा खतरा सम्बन्धमा २४/७ भरी नै अनुगमन गर्न केन्द्रको कुनै महाशाखा वा शाखालाई जिम्मेवारी प्रदान गर्ने,

(घ) राष्ट्रिय सुरक्षा, प्रतिरक्षा, अर्थतन्त्र, अन्तर्राष्ट्रिय सम्बन्ध, सार्वजनिक स्वास्थ्य, सार्वजनिक शान्ति र व्यवस्था वा सार्वजनिक सुरक्षा, वा अन्य कुनै अत्यावश्यक सेवालाई खतरामा पार्न सक्ने साईबर सुरक्षाका घटनाको प्रतिरक्षा गर्ने,

(ङ) संवेदनशील सूचना पूर्वाधारको पहिचान गर्ने र तोक्ने, तथा संवेदनशील सूचना पूर्वाधारका धनीले अवलम्बन गरेको साईबर सुरक्षा अनुगमन गर्ने,

(च) साईबर सुरक्षा सम्बन्धी मापदण्ड बनाउने,

(छ) अन्तर्राष्ट्रिय स्तरमा साईबर सुरक्षाका विषयहरुमा सरकारको प्रतिनिधित्व गर्ने,

(ज) देशभित्र साईबर सुरक्षा सम्बन्धी उद्योगको विकास तथा प्रवर्धन गर्ने,

(झ) अनुमतिपत्र तथा साईबर सुरक्षा सेवा प्रदायकका सम्बन्धमा मापदण्ड तयार गर्ने,

(ञ) साईबर सुरक्षा सम्बन्धी कम्प्युटरको हार्डवयर तथा सफ्टवयर सम्बन्धमा मापदण्ड निर्धारण गर्ने,

(ट) साईबर सुरक्षा क्षेत्रमा काम गर्ने व्यक्तिहरुको व्यवसायिक स्तर प्रतिस्पर्धात्मक बनाउने,

(ठ) साईबर सुरक्षा सम्बन्धी प्रविधिको विकास तथा अनुसन्धान तथा विकासलाई प्रोत्साहन गर्ने वा आवश्यकता अनुसार त्यस्ता कार्य गर्न विश्व विद्यालयहरुसँग सहकार्य गर्ने,

(ड) साईबर सुरक्षाको महत्व र आवश्यकताका सम्बन्धमा सचेतना अभिबृद्धि गर्ने,

(ढ) साईबर सुरक्षा सेवा प्रदायक तथा अडिटरलाई अनुमतिपत्र प्रदान गर्ने,

(ण) केन्द्रको वार्षिक आयव्ययको विवरण तथा वार्षिक प्रतिवेदन तयार गरी स्वीकृतिको लागि समिति समक्ष पेश गर्ने,

(त) साईबर सुरक्षा सम्बन्धमा राष्ट्रिय तथा अन्तर्राष्ट्रिय संस्थासँग आवश्यक समन्वय तथा सहकार्य गर्ने,

(थ) साईबर सुरक्षा सम्बन्धी गोष्ठि, तालीम आदि संचालन गर्ने,

(द) साईबर सुरक्षा सम्बन्धमा प्रदेश सरकार, स्थानीय तह तथा अन्य सम्बद्ध निकाय बीच आवश्यक समन्वयय गर्ने,

(ध) साईबर सुरक्षा सम्बन्धमा आई पर्ने अन्य आवश्यक कार्य गर्ने गराउने ।

परिच्छेद- ३

राष्ट्रिय साईबर सुरक्षा समितिको गठन, काम, कर्तव्य र अधिकार

६. **समितिको गठन**: केन्द्रको उद्देश्य प्राप्ति तथा केन्द्रको समग्र काम कारबाहीको संचालन, रेखदेख र प्रवन्ध गर्न राष्ट्रिय साईबर सुरक्षा समिति नामको एक समिति रहनेछ ।

(२) उपदफा (१) बमोजिमको समितिमा देहायका सदस्य रहनेछन्:-

(क) मन्त्री, सूचना, प्रविधि तथा संचार मन्त्रालय -अध्यक्ष

(ख) सचिव, मन्त्रालय -सदस्य

(ग) सचिव, गृह मन्त्रालय -सदस्य

(घ) सचिव, विज्ञान तथा प्रविधि मन्त्रालय -सदस्य

(ङ) सचिव, रक्षा मन्त्रालय -सदस्य

(च) सचिव, अर्थ मन्त्रालय -सदस्य

(छ) अध्यक्ष, नेपाल दुर संचार प्राधिकरण -सदस्य

(ज) सूचना प्रविधि, साईवर सुरक्षा विज्ञ, सूचना प्रविधि सम्बन्धी सेवा प्रदायक संस्थाहरु मध्येबाट नेपाल सरकारले मनोनयन गरेका तीन जना -सदस्य

(झ) केन्द्रको प्रमुख कार्यकारी अधिकृत -सदस्य सचिव

(३) उपदफा (२) को खण्ड (झ) बमोजिमका सदस्यहरुको पदावधि चार वर्षको हुनेछ ।

७. **अयोग्यता**: देहायको व्यक्ति दफा ६ को उपदफा (२) को खण्ड (झ) बमोजिमको सदस्य पदमा नियुक्ति हुन वा पदमा बहाल रहन योग्य हुने छैन:-

(क) गैरनेपाली नागरिक,

(ख) ४० वर्ष नपुगेको र ६० वर्ष उमेर पूरा गरेको,

(ग) विदशी मुलुकको आवासीय अनुमति लिएको,

(घ) भ्रष्टाचार, जवरजस्ति करणी, मानव बेचविखन तथा ओसार पसार, लागू औषध कारोवार, सम्पत्ति शुद्धिकरण, राहदानी, दुरुपयोग, अपहरण सम्बन्धी कसूर वा नैतिक पतन देखिने फौजदारी कसूरमा सजाय पाएको,

(ङ) प्रचलित कानून बमोजिम कालोसूचीमा परेको वा त्यस्तो सूचीबाट फुकुवा भएको मितिले तीन वर्ष पूरा नभएको,

(च) साहुको ऋण तिर्न नसकि दामासाहीमा परेको,

(छ) कुनै राजनैतिक दलको सदस्य वा पदाधिकारी भएको ।

८. **सदस्यको पद रिक्त हुने अवस्था**: दफा ६ को उपदफा (२) को खण्ड (झ) बमोजिम मनोनित सदस्यको पद देहायको अवस्थामा रिक्त भएको मानिनेछः-

(क) निजले मनोनयन गर्ने निकाय समक्ष लिखित राजिनामा दिएमा,

(ख) निजको पदावधि समाप्त भएमा,

(ग) निज साहुको दामासाहीमा परेमा,

(घ) निजले भ्रष्टाचार, जवरजस्ति करणी, मानव बेचविखन तथा ओसार पसार, लागू औषध कारोबार, सम्पत्ति सुद्धिकरण, राहदानी दुरुपयोग, अपहरण समबन्धी कसूर वा नैतिक पतन देखिने फौजदारी कसूरमा सजाय पाएमा,

(ङ) निज विना सूचना लगातार तीन पटकसम्म समितिको बैठकमा अनुपस्थित भएमा,

(च) निजको मृत्यु भएमा ।

९. **रिक्त स्थानको पूर्ति**: कार्यकारी समितिको दफा ६ को खण्ड (ज) बमोजिमको मनोनित सदस्यको पद कुनै कारणबाट रिक्त हुन आएमा निज पहिले जुन तरिकाबाट मनोनयन भएको हो सोही तरिकाबाट मनोनयन गरी रिक्त पद पूर्ति गरिनेछ ।

१०. **समितिको काम, कर्तव्य र अधिकार**: (१) यस ऐनमा अन्यत्र लेखिएको काम, कर्तव्य र अधिकारको अतिरिक्त समितिको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) साईबर सुरक्षा सम्बन्धी रणनीति, नीति निर्माण गर्न नेपाल सरकारलाई परामर्श दिने,

(ख) केन्द्रको बजेट तथा कार्यक्रम स्वीकृत गर्ने,

(ग) केन्द्रको वार्षिक आय व्ययको विवरण तथा वार्षिक प्रतिवेदन स्वीकृत गर्ने,

(घ) केन्द्रलाई मार्गदर्शन गर्ने तथा आवश्यक निर्देशन दिने,

(ङ) केन्द्रबाट भए गरेका कामको सुपरीवेक्षण तथा मूल्याङ्कन गर्ने,

(च) शैक्षिक संस्था, विश्वविद्यालय तथा तालीम केन्द्रको पाठ्यक्रममा साईबर सुरक्षा सम्बन्धी विषय समावेश गर्न सिफारिस गर्ने,

(छ) तोकिए बमोजिमका अन्य कार्य गर्ने ।

११. **समितिको बैठक र निर्णय**: (१) समितिको बैठक कम्तिमा एक वर्षमा चार पटक बस्नेछ र दुई बैठक बीचको फरक चार महिना भन्दा बढी हुने छैन ।

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

(३) उपदफा (२) मा जुनसुकै कुरा लेखिएको भए तापनि समितिका कम्तिमा पच्चिस प्रतिशत सदस्यले कार्यकारी समितिको बैठक बोलाउन अनुरोध गरेमा अध्यक्षले त्यस्तो लिखित अनुरोध प्राप्त भएको मितिले सात दिन भित्र समितिको बैठक बोलाउनु पर्नेछ ।

(४) समितिका कूल सदस्य संख्याको पचास प्रतिशत भन्दा बढी सदस्य उपस्थित भएमा बैठकको लागि गणपूरक संख्या पुगेको मानिनेछ ।

(५) समितिको बैठकको अध्यक्षता अध्यक्षले गर्नेछ र निजको अनुपस्थितिमा उपस्थित सदस्यहरुले आफू मध्येबाट छानेको सदस्यले बैठकको अध्यक्षता गर्नेछ ।

(६) समितिको बैठकमा बहुमतको राय समितिको निर्णय हुनेछ र मत बराबर भएमा अध्यक्षता गर्ने व्यक्तिले निर्णायक मत दिनेछ ।

(७) समितिको निर्णय समितिको सदस्य सचिवले प्रमाणित गर्नेछ ।

(८) समितिको बैठक सम्बन्धी अन्य कार्यविधि समिति आफैँले निर्धारण गरे बमोजिम हुनेछ ।

परिच्छेद- ४

केन्द्रको कोष र लेखा परीक्षण

१२. **केन्द्रको कोष**: (१) केन्द्रको आफ्नो एउटा छुट्टै कोष हुनेछ ।

(२) उपदफा (१) बमोजिमको कोषमा देहायका रकम रहनेछन्:-

(क) नेपाल सरकारबाट प्राप्त रकम,

(ख) विदेशी सरकार, अन्तर्राष्ट्रिय संघ संस्थाबाट अनुदान वा सहयोग स्वरुप प्राप्त रकम, यस खण्ड बमोजिम अनुदान वा सहयोग प्राप्त गर्न नेपाल सरकारको पूर्व स्वीकृति लिनु पर्नेछ,

(ग) अनुमतिपत्र वा अनुमतिपत्र नविकरण दस्तुर बापत प्राप्त रकम,

(घ) अन्य कुनै स्रोतबाट प्राप्त रकम ।

(३) केन्द्रको सम्पूर्ण खर्च उपदफा (१) बमोजिमको कोषबाट व्यहोरिनेछ ।

(४) केन्द्रको कोषमा रहने रकम नेपालभित्रको कुनै बैंक वा वित्तीय संस्थामा खाता खोली जम्मा गरिनेछ र त्यस्तो खाताको संचालन तोकिए बमोजिम हुनेछ ।

१३. **लेखा र लेखा परीक्षण**: (१) केन्द्रको आय व्ययको लेखा प्रचलित कानून बमोजिम राखिनेछ ।

(२) केन्द्रको आय व्ययको लेखापरीक्षण महालेखा परीक्षकको कार्यालयले गर्नेछ ।

(३) नेपाल सरकारले चाहेमा जुनसुकै बखत केन्द्रको लेखा तथा सोसँग सम्बन्धित कागजात जाँच्न वा जाँच्न लगाउन सक्नेछ ।

परिच्छेद- ५

संवेदनशील सूचना पूर्वाधार

१४. **संवेदनशील सूचना पूर्वाधार तोक्ने**: (१) यस ऐनको प्रयोजनको लागि देहायको कुरामा केन्द्र सन्तुष्ट भएमा कम्प्युटर वा कम्प्युटर प्रणालीको धनीलाई लिखित सूचना दिएर त्यस्तो कम्प्युटर वा कम्प्युटर प्रणाली संवेदनशील सूचना पूर्वाधार भित्र पर्ने भनी तोक्न लगाउन सक्नेछ:

(क) कम्प्युटर वा कम्प्युटर प्रणाली अविच्छिन्न रुपमा अत्यावश्यक सेवा पुऱ्याउन आवश्यक रहेको र त्यस्तो कम्प्युटर र कम्प्युटर प्रणालीमा क्षति पुग्न गएमा वा कुनै किसिमको सम्झौता गरिएमा अत्यावश्यक सेवाको उपलब्धतामा प्रभाव पर्न सक्ने,

(ख) त्यस्तो कम्प्युटर वा कम्प्युटर प्रणाली पूर्ण वा आंशि रुपमा नेपालमा रहेको ।

(२) उपदफा (१) बमोजिम जारी गरिएको सूचनामा देहायका कुरा समेत उल्लेख गर्नु पर्नेछ:-

(क) संवेदनशील सूचना पूर्वाधारको रुपमा तोक्न गईरहेको कम्प्युटर वा कम्प्युटर प्रणाली पहिचान गर्ने,

(ख) संवेदनशील सूचना पूर्वाधारको रुपमा तोकिएको कम्प्युटर वा कम्प्युटर प्रणालीको धनी पहिचान गर्ने,

(ग) संवेदनशील सूचना पूर्वाधारको रुपमा तोकिए पछि यस ऐन बमोजिम कम्प्युटर वा कम्प्युटर प्रणालीका धनीको काम तथा दायित्व के हुने भन्ने सम्बन्धमा सम्बन्धित धनीलाई जानकारी दिने,

(घ) संवेदनशील सूचना पूर्वाधार निरीक्षण गर्न तोकिएको अधिकृतको नाम तथा सम्पर्क विवरण उपलब्ध गराउने,

(ङ) कुनै कम्प्युटर वा कम्प्युटर प्रणाली संवेदनशील सूचना पूर्वाधार तोकिएकोमा चित्त नबुझे मन्त्रालय समक्ष गुनासो राख्न पाउने कुरा कम्प्युटर वा कम्प्युटर प्रणालीका धनीलाई जानकारी दिने,

(३) उपदफा (१) बमोजिम तोकिएको अवधी पाँच वर्षको लागि हुनेछ ।

(४) उपदफा (१) बमोजिमको सूचना प्राप्त गर्ने कुनै पनि व्यक्तिले देहायका कुरा उल्लेख गरी उपदफा (५) बमोजिम गर्न केन्द्र समक्ष अनुरोध गर्न सक्नेछः-

(क) कम्प्युटर वा कम्प्युटर प्रणालीको संचालनमा कुनै प्रभावकारी नियन्त्रण नभएको कारणले यस खण्ड बमोजिमका शर्त पालना गर्न नसक्ने वा कम्प्युटर वा कम्प्युटर प्रणालीमा परिवर्तन गर्ने अधिकार नभएको कुरा,

(ख) कम्प्युटर वा कम्प्युटर प्रणाली संचालनमा अर्को व्यक्तिको प्रभावकारी नियन्त्रण रहेको र निजले मात्र परिवर्तन कार्यान्वयनमा ल्याउन नसक्ने कुरा ।

(५) उपदफा (४) बमोजिम पेश भएको विवरणको सम्बन्धमा केन्द्र सन्तुष्ट भएमा उपदफा (१) बमोजिम जारी भएको सूचना संशोधन गरी सोको जानकारी सम्बन्धित व्यक्तिलाई दिनु पर्नेछ ।

(६) संवेदनशील सूचना पूर्वाधार नेपाल सरकार, प्रदेश सरकार वा स्थानीय तहको स्वामित्वमा रहेको भएमा यस ऐनको प्रयोजनको लागि त्यस्ता निकायको प्रमुख संवेदनशील सूचना पूर्वाधारको धनीको रुपमा मानिनेछ ।

(७) यस ऐन बमोजिम जारी गरिएको सूचना सबैले थाहा पाउने गरी केन्द्रको वेभ साईटमा राख्नु पर्नेछ ।

१५. **जानकारी माग गर्न सक्ने**: (१) केन्द्रले कुनै कम्प्युटर वा कम्प्युटर प्रणालीले संवेदनशील सूचना पूर्वाधार सम्बन्धी शर्त पालना गरेको छ वा छैन भन्ने कुरा सुनिश्चित गर्न कम्प्युटर वा कम्प्युटर प्रणालीलाई नियन्त्रण गर्ने व्यक्तिसँग तोकिए बमोजिमको ढाँचामा जानकारी माग गर्न सक्नेछ ।

(२) उपदफा (१) बमोजिम जारी गरिने सूचनामा केन्द्रले देहायका कुरा माग गर्न सक्नेछः

(क) सेवा प्रदान गर्न प्रयोगमा ल्याईएको कम्प्युटर वा कम्प्युटर प्रणालीको काम सम्बन्धी जानकारी,

(ख) कुन व्यक्ति वा व्यक्तिहरुको लागि सेवा प्रदान गरिएको हो त्यस्ता व्यक्तिको जानकारी,

(ग) कम्प्युटर वा कम्प्युटर प्रणालीको डिजाईन सम्बन्धी जानकारी,

(घ) कम्प्युटर वा कम्प्युटर प्रणालीले संवेदनशील सूचना पूर्वाधार सम्बन्धी शर्तहरु पालना गरको छ वा छैन भन्ने कुरा सुनिश्चित गर्न आवश्यक पर्ने अन्य जानकारीहरु ।

१६. **संवेदनशील सूचना पूर्वाधारबाट हटाउन सक्ने**: कम्प्युटर वा कम्प्युटर प्रणाली संवेदनशील सूचना पूर्वाधारको आवश्यक मापदण्ड भित्र पर्दैन भन्ने कुरामा केन्द्र सन्तुष्ट भएमा केन्द्रले त्यस्तो कम्प्युटर वा कम्प्युटर प्रणालीलाई कुनैपनि समयमा संवेदनशील सूचना पूर्वाधारको सूचीबाट हटाउन सक्नेछ ।

१७. **संवेदनशील सूचना पूर्वाधार सम्बन्धी सूचना दिनु पर्ने**: (१) केन्द्रले संवेदनशील सूचना पूर्वाधारका धनीलाई सूचना जारी गरी तोकिए बमोजिमको ढाँचा र समय भित्र सूचनामा उल्लेख गरिएका देहायका विषयमा जानकारी माग गर्न सक्नेछ:-

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

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

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

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

(२) उपदफा (१) बमोजिम सूचना दिईएको संवेदनशील सूचना पूर्वाधारको धनीलाई आम नागरिकको हैसियतले अन्य प्रचलित नेपाल कानूनले कुनै प्रकारको जानकारी दिन कर नलाग्ने गरी छुट दिएको रहेछ भने निज त्यस्तो जानकारी उपलब्ध गराउन बाध्य हुने छैन ।

(३) उपदफा (१) बमोजिमको जानकारी केन्द्रलाई दिईसके पछि संवेदनशील सूचना पूर्वाधार धनीको तर्फबाट संवेदनशील सूचना पूर्वाधारको डिजाईन, कन्फिगुरेसन, सुरक्षा वा संचालनमा तात्विक परिवर्तन गरिएको भएमा तीस दिनभित्र सोको जानकारी केन्द्रलाई दिनु पर्नेछ ।

१८. **निर्देशन दिन तथा मापदण्ड बनाई लागू गर्न सक्ने**: (१) केन्द्रले समय समयमा संवेदनशील सूचना पूर्वाधारको साईबर सुरक्षा सम्बन्धमा संवेदनशील सूचना पूर्वाधारका धनीले अवलम्बन गर्नु पर्ने उपायहरुका सम्बन्धमा निर्देशन दिन तथा मापदण्ड बनाई लागू गर्न सक्नेछ ।

(२) केन्द्रले उपदफा (१) बमोजिम दिएको निर्देशन तथा लागू गरिएको मापदण्ड आवश्यकता अनुसार कुनै पनि समयमा संशोधन वा खारेज गर्न सक्नेछ ।

(३) केन्द्रले उपदफा (१) बमोजिम दिएको निर्देशन वा तयार गरी लागू गरेको मापदण्ड सरोकारवाला सबैले थाहा पाउन सक्ने गरी प्रकाशन गर्नु पर्नेछ ।

(४) उपदफा (१) बमोजिम केन्द्रले दिएको निर्देशन वा लागू गरेको मापदण्ड संवेदनशील सूचना पूर्वाधारका धनीले पालना गर्नु पर्नेछ ।

१९. **जानकारी दिनु पर्ने**: (१) संवेदनशील सूचना पूर्वाधारको धनी परिवर्तन भएमा सम्बन्धित व्यक्तिले त्यसरी परिवर्तन भएको सात दिनभित्र केन्द्रलाई जानकारी दिनु पर्नेछ ।

स्पष्टिकरण: यस दफाको प्रयोजनको लागि सम्बन्धित व्यक्ति भन्नाले त्यस्तो संवेदनशील सूचना पूर्वाधार हस्तान्तरण हुनु भन्दा अघिको धनी सम्झनु पर्छ ।

२०. **साईबर सुरक्षाका घटनाको बारेमा सूचना दिनु पर्ने**: (१) संवेदनशील सूचना पूर्वाधारका धनीले साईबर सुरक्षाका घटना घटेमा त्यस्तो घटना घट्ने वित्तिकै केन्द्रलाई तोकिएको ढाँचामा देहायका कुराका सम्बन्धमा जानकारी उपलब्ध गराउनु पर्नेछ:-

(क) संवेदनशील सूचना पूर्वाधार सम्बन्धमा तोकिए बमोजिमको साईबर सुरक्षा घटना,

(ख) संवेदनशील पूर्वाधार सूचना प्रणालीको धनीले आफ्नो नियन्त्रणमा रहेको संवेदनशील पूर्वाधार सूचना प्रणालीसँग संचार आदान प्रदान गर्ने गरी जोडिएको कुनै कम्प्युटर वा कम्प्युटर प्रणालीसँग सम्बन्धीत तोकिएको साईबर सुरक्षा घटना,

(ग) संवेदनशील सूचना पूर्वाधारसँग सम्बन्धित साईबर सुरक्षा सम्बन्धी अन्य कुनै किशिमको घटना ।

(२) संवेदनशील सूचना पूर्वाधारको धनीले त्यस्तो संवेदनशील सूचना पूर्वाधारसँग सम्बन्धित साईबर सुरक्षा खतरा वा घटना पत्ता लगाउन संवेदनशील पूर्वाधार सूचना प्रणाली संयन्त्रको स्थापना तथा सो सम्बन्धी कार्यविधि निर्धारण गर्नु पर्नेछ ।

२१. **साईबर सुरक्षा अडिट तथा जोखिम मूल्याङ्कन गराउनु पर्ने**: (१) संवेदनशील सूचना पूर्वाधारको धनीले प्रत्येक दुई वर्षमा संवेदनशील सूचना पूर्वाधारको साईबर सुरक्षा अडिट तथा कम्तिमा प्रत्येक वर्ष संवेदनशील सूचना पूर्वाधारको जोखिम मूल्याङ्कन गराउनु पर्नेछ ।

तर साईबर सुरक्षा अडिट गराएको वर्ष संवेदनशील सूचना पूर्वाधारको अडिट गरिएको वर्ष संवेदनशील सूचना पूर्वाधारको जोखिम मूल्याङ्कन गराउनु पर्ने छैन ।

(२) संवेदनशील सूचना पूर्वाधारको धनीले उपदफा (१) बमोजिम गराएको साईबर सुरक्षाको अडिट तथा जोखिम मूल्याङ्कन प्रतिवेदनको प्रतिलिपि तीस दिन भित्र केन्द्र समक्ष पेश गर्नु पर्नेछ ।

(३) उपदफा (१) बमोजिम साईबर सुरक्षा अडिट गर्दा साईबर सुरक्षाका कुनै पक्षमा सन्तोषजनक किशिमले अडिट गरिएको छैन भन्ने कुरामा केन्द्र सन्तुष्ट भएमा केन्द्रले त्यस्ता छुट भएका पक्षका सम्बन्धमा अडिट गराउन निर्देशन दिन सक्नेछ ।

(४) संवेदनशील सूचना पूर्वाधारको धनीले यस ऐन वा यस ऐन अन्तर्गत बनेको नियमावली वा मापदण्ड पालना गरेको छैन वा दफा १९ बमोजिम दिएको जानकारी भ्रामक, गलत वा झुट्टा हो भन्ने कुरामा केन्द्र सन्तुष्ट भएमा केन्द्रले साईबर सुरक्षा अडिट गराउन अर्को अडिटर तोकि पठाउने छ र त्यसरी अडिट गर्दा लागेको शुल्क सम्बन्धित संवेदनशील सूचना पूर्वाधारको धनीले व्यहोर्नु पर्नेछ ।

(५) उपदफा (२) बमोजिम पेश गरिएको साईबर सुरक्षा जोखिम मूल्याङ्कन प्रतिवेदनबाट त्यस्तो मूल्याङ्कन गर्ने कार्य सन्तोषजनक तरिकाले भएको छैन भन्ने कुरामा केन्द्र सन्तुष्ट भएमा केन्द्रले संवेदनशील सूचना पूर्वाधारको धनीलाई संवेदनशील सूचना पूर्वाधारको जोखिम मूल्याङ्कन पुनः गराउन निर्देशन दिनेछ वा संवेदनशील सूचना पूर्वाधारको जोखिम मूल्याङ्कन गर्न साईवर सुरक्षा सेवा प्रदायकलाई नियुक्ति गरी पठाउनेछ र यसरी पठाउँदा लागेको खर्च संवेदनशील सूचना पूर्वाधारको धनीले व्यहोर्नु पर्नेछ ।

(६) संवेदनशील सूचना पूर्वाधारको धनीले दफा १४ को उपदफा (५) बमोजिम डिजाईन, कन्फिगुरेसन, सुरक्षा वा संवेदनशील सूचना पूर्वाधारको संचालनमा तात्विक परिवर्तन गरेको सम्बन्धमा केन्द्र समक्ष पेश गरिएको जानकारी उपर केन्द्र सनतुष्ट हुन नसकेमा केन्द्रले पुनः अडिट गराउन वा साईबर सुरक्षा जोखिम मूल्याङ्कन गराउन आदेश दिनेछ ।

(७) संवेदनशील सूचना पूर्वाधारको धनीले उपयुक्त कारण बेगर उपदफा (१) वा यस दफा बमोजिम केन्द्रले दिएको निर्देशनको अवज्ञा गर्न वा उपदफा (४) बमोजिम अडिट गर्न वा जोखिम मूल्याङ्कन गर्न अवरोध गर्नु हुँदैन ।

परिच्छेद- ६

साईबर सुरक्षा जोखिम तथा घटनाको प्रतिरक्षा सम्बन्धी व्यवस्था

२२. **साईबर सुरक्षाका घटनाको छानविन तथा रोकथाम**: (१) साईबर सुरक्षा जोखिम वा घटना सम्बन्धी जानकारी प्राप्त भएमा केन्द्रले साईबर सुरक्षाको जोखिम वा घटनाका बारेमा समिक्षा वा मूल्याङ्कन गर्न साईबर सुरक्षा अधिकृत तोक्न सक्नेछ र निजलाई देहायका अधिकार सहित उपदफा (२) मा उल्लेख गरिएको अधिकार हुनेछः-

(क) साईबर सुरक्षा खतरा वा घटनाको सम्भावित असर वा असरको मूल्याङ्कन गर्ने,

(ख) साईबर सुरक्षाको घटनाबाट उत्पन्न क्षति रोक्ने वा थप क्षति हुन नदिने,

(ग) भविश्यमा यस प्रकारका साईबर सुरक्षा खतरा वा घटना हुन नदिने ।

(२) उपदफा (१) मा उल्लिखित अधिकार अन्तर्गत देहायका अधिकार समावेश हुनेछन्:-

(क) साईबर सुरक्षा घटनाको प्रतिरक्षा गर्न खटाईएको अधिकृतले उल्लेख गरे बमोजिम कुनै व्यक्तिलाई तोकिएको स्थान वा समयमा साईबर सुरक्षामाथिको खतरा वा घटनाका सम्बन्धमा सोधिने प्रश्नको जवाफ दिन लिखित सूचना दिई उपस्थित गराउन सक्ने,

(ख) छानविनको क्रममा कुनै कुरा सम्बन्धित देखिएमा लिखित सूचना दिएर कुनै पनि व्यक्तिलाई निजको कब्जामा रहेको भौतिक वा विद्युतीय अभिलेख वा दस्तावेजको प्रतिलिपि पेश गर्न लगाउन सक्ने,

(ग) खण्ड (ख) मा समावेश गरिएका सामग्रीहरु विना शुल्क निरीक्षण गर्न वा प्रतिलिपि लिन सक्ने,

(घ) घटनाको बारेमा थाहा पाएको कुनै व्यक्तिसँग घटनाको तथ्यको बारेमा जानकारी लिन सक्ने ।

(३) घटना प्रतिरक्षा गर्ने अधिकृतले दफा २ को उपदफा (ख) मा उल्लिखित सूचनामा देहायका कुरा उल्लेख गर्नु पर्नेछः-

(क) कुनै अभिलेख, दस्तावेज वा प्रतिलिपि वा कुनै जानकारी उपलब्ध गराउने समय र स्थान,

(ख) खण्ड (क) मा उल्लेख गरिएका सामग्री उपलब्ध गराउने तरिका ।

(४) यस दफा बमोजिम बुझिएको व्यक्तिको भनाई देहाय बमोजिम गरी राख्नु पर्नेछः-

(क) लेखबद्ध गर्ने,

(ख) लेखबद्ध गरिएको कुरा सम्बन्धित व्यक्तिलाई पढेर सुनाउने,

(ग) यदि कुनै व्यक्ति नेपाली भाषा नबुझ्ने रहेछ भने निजले बुझ्ने भाषामा भन्नको लागि दोभाषे राख्ने,

(घ) आवश्यक भएमा लेखबद्ध गरिएको कुरामा आवश्यक सुधार गरी त्यस्तो व्यक्तिको दस्तखत गराउने ।

(५) सम्बन्धित व्यक्तिले यस दफा बमोजिम दिईएको आदेशको पालना गर्नु पर्नेछ ।

२३. **गम्भिर प्रकृतिका साईबर सुरक्षाका घटना नियन्त्रण**: (१) साईबर सुरक्षा खतरा वा घटना सम्बन्धी जानकारी प्राप्त भएपछि त्यस्तो जोखिम वा घटनाबाट उपदफा (३) बमोजिमको गाम्भिर्यताको सीमा (थ्रेशहोल्ड) पूरा गरेको छ भन्ने कुरामा केन्द्र सन्तुष्ट भएमा वरिष्ठ दर्जाको साईबर सुरक्षा अधिकृतलाई साईबर सुरक्षाको खतरा वा घटनाका बारेमा उपदफा (२) मा बमोजिमका अधिकारका साथै देकायका अधिकार प्रदान गर्नेछः-

(क) साईबर सुरक्षा खतरा वा घटनाको सम्भावित असर वा असरको मूल्याङ्कन गर्ने,

(ख) साईबर सुरक्षा खतरा हटाउने वा साईबर सुरक्षा घटनाबाट उत्पन्न क्षति रोक्ने वा अरु क्षति हुन नदिने,

(ग) अरु साईबर सुरक्षा खतरा वा घटना हुन नदिने ।

(२) उपदफा (१) मा उल्लिखित अधिकार अन्तर्गत देहायका अधिकार समावेश हुनेछन्:-

(क) साईबर घटनाको प्रतिरक्षा गर्न उपदफा (१) बमोजिम खटाईएको अधिकृतले कुनै व्यक्तिलाई तोकिएको स्थान वा समयमा साईबर सुरक्षा खतरा वा घटनाका सम्बन्धमा सोधिने प्रश्नको जवाफ दिन लिखित सूचना दिई उपस्थित गराउन सक्ने,

(ख) छानविनको क्रममा कुनै कुरा सम्बन्धित देखिएमा लिखित सूचना दिएर कुनै पनि व्यक्तिलाई निजको कब्जामा रहेको भौतिक वा विद्युतीय अभिलेख, वा दस्तावेज वा अभिलेख वा कागजातको प्रतिलिपि आफू समक्ष पेश गर्न लगाउन सक्ने,

(ग) खण्ड (ख) मा समावेश गरिएका सामग्रीहरु सम्बन्धित व्यक्तिले आफू समक्ष पेश गराउँदा कुनै शुल्क लिन नपाउने ।

(घ) घटनाको बारेमा थाहा पाउने कुनै व्यक्तिसँग घटनाको तथ्यको बारेमा जानकारी लिन सक्ने ।

(३) कुनै पनि साईबर सुरक्षा खतरा वा घटनाले देहायका कुरा पूरा गरेको भएमा गाम्भिर्यताको सीमा (थ्रेसहोल्ड) पूरा गरेको मानिनेछ:-

(क) संवेदनशील सूचना पूर्वाधारमा ठूलो क्षतिको खरता उत्पन्न गराउने भएमा,

(ख) अत्यावश्यक वस्तुको आपूर्तिमा खलल पुऱ्याउने खतरा उत्पन्न गराउने भएमा,

(ग) नेपालको राष्ट्रिय सुरक्षा, प्रतिरक्षा, वैदेशिक सम्बन्ध, अर्थतन्त्र, सार्वजनिक स्वास्थ्य, सार्वजनिक सुरक्षा, शान्ति र व्यवस्थामा खतरा उत्पन्न गराउने भएमा,

(घ) संवेदनशील सूचना पूर्वाधार नभए पनि पनि साईबर सुरक्षाको घटना गम्भिर प्रकृतिको भई धेरै कम्प्युटर वा कम्प्युटर प्रणाली वा सूचनाको महत्व उपर खतरा उत्पन्न गराउने भएमा ।

(४) घटना प्रतिरक्षा गर्ने अधिकृतले दफा २ को खण्ड (ख) बमोजिमको सूचनामा देहायका कुरा उल्लेख गर्नु पर्नेछ:-

(क) कुनै अभिलेख, कागजात वा प्रतिलिपि वा कुनै जानकारी उपलब्ध गराउने समय र स्थान,

(ख) खण्ड (क) मा बमोजिमका सामग्री उपलब्ध गराउने तरिका ।

(५) यस दफा बमोजिम बुझिएको व्यक्तिको भनाई देहाय बमोजिम गरी राख्नु पर्नेछः-

(क) लेखबद्ध गर्ने,

(ख) लेखबद्ध गरिएको भनाई सम्बन्धित व्यक्तिलाई पढेर सुनाउने,

(ग) यदि कुनै व्यक्ति नेपाली भाषा नबुझ्ने रहेछ भने निजले बुझ्ने भाषामा भन्नको लागि दोभाषे राख्ने,

(घ) आवश्यक भएमा बुझिएको व्यक्तिको भनाईलाई आवश्यक सुधार गरी त्यस्तो व्यक्तिको दस्तखत गराउने ।

(६) यो दफा बमोजिम दिईएको आदेश सम्बन्धित सबैले पालना गर्नु पर्नेछ ।

२४. **साईबर सुरक्षा घटना प्रतिरक्षाका लागि खटिएको अधिकृतले आफ्नो परिचयपत्र देखाउनु पर्नेः** साईबर सुरक्षा घटनाको छानविन, मूल्याङ्कन वा प्रतिरक्षाको लागि खटिएको साईबर सुरक्षा अधिकृतले त्यस्तो घटनाबाट पीडित व्यक्तिले माग गरेको खण्डमा आफ्नो परिचयपत्र देखाउनु पर्नेछ ।

२५. **साईबर सुरक्षा प्रविधि विज्ञ नियुक्ति गर्न सक्नेः** (१) केन्द्रले साईबर सुरक्षा घटना छानविन गर्न खटाईएको कुनै अधिकृतलाई छानविन कार्यमा सहयोग गर्न निश्चित अवधि तोकि देहायको कुनै व्यक्तिलाई साईबर सुरक्षा प्रविधि विज्ञको रुपमा नियुक्ति गर्न सक्नेछः-

(क) सरकारी निकायको कुनै अधिकृत,

(ख) तोकिए बमोजिमको योग्यता पुगेको कुनै व्यक्ति,

(२) उपदफा (१) बमोजिम नियुक्त साईबर सुरक्षा प्रविधि विज्ञले साईबर सुरक्षा घटना छानविन गर्न खटिएको अधिकृतलाई आवश्यक पर्ने प्राविधिक परामर्श उपलब्ध गराउनु पर्नेछ ।

(३) उपदफा (१) बमोजिम नियुक्त साईबर सुरक्षा प्रविधि विज्ञको काम सन्तोषजनक नभएमा केन्द्रले निजलाई जुनसुकै समयमा हटाउन सक्नेछ ।

(४) केन्द्रले उपदफा (१) बमोजिम नियुक्त साईबर सुरक्षा प्रविधि विज्ञको नाममा नियुक्ति भएको अवधिभर बहाल रहने गरी परिचय पत्र जारी गर्नु पर्नेछ ।

(५) उपदफा (१) बमोजिम नियुक्त साईबर सुरक्षा प्रविधि विज्ञले नियुक्ति अवधि समाप्त भएपछि आफूले प्राप्त गरेको परिचयपत्र केन्द्रलाई फर्काउनु पर्नेछ ।

२६. **साईबर सुरक्षा आपतकालीन उपायहरुको अवलम्बनः** (१) यस ऐनको दफा २ को खण्ड (क) तथा अनुसूची-१ मा उल्लिखित संवेदनशील सूचना पूर्वाधारसँग सम्बन्धित कम्प्युटर वा कम्प्युटर प्रणालीमा तथा अत्यावश्यक सेवाका सामग्री, राष्ट्रिय सुरक्षा, प्रतिरक्षा, मित्र

राष्ट्रहरुसँगको सम्बन्ध, अर्थतन्त्र, सार्वजनिक स्वास्थ्य, सार्वजनिक सुरक्षा वा शान्ति र व्यवस्थामा गम्भिर तथा आसन्न जोखिम छ भन्ने लागेमा त्यस्ता कुरा रोक्न, पत्ता लगाउन, जुध्न केन्द्रले कुनै कम्प्युटर वा कम्प्युटर प्रणाली वा कुनै वर्गमा पर्ने कम्प्युटर वा कम्प्युटर प्रणालीमा आवश्यक पर्ने उपायहरु अवलम्बनय गर्न वा त्यस्ता उपायहरु पालना गर्न लगाउन कुनै साईबर सुरक्षा अधिकृतलाई आदेश दिन सक्नेछ ।

(२) उपदफा (१) बमोजिम खटिएको अधिकृतले साईबर सुरक्षा खतरा पत्ता लगाउन वा प्रतिरक्षा गर्ने प्रयोजनको लागि अर्को कुनै व्यक्तिलाई देहायका कुरा उपलब्ध गराउन निर्देशन दिन सक्नेछः-

(क) कम्प्युटर, कम्प्युटर प्रोग्राम वा कम्प्युटर प्रणालीको डिजाईन, कन्फिगुरेसन वा संचालन सम्बन्धी जानकारी,

(ख) कम्प्युटर, कम्प्युटर प्रोग्राम वा कम्प्युटर प्रणालीको साईबर सुरक्षा सम्बन्धी जानकारी,

(३) उपदफा (१) बमोजिम खटिएको व्यक्ति आफूले दिएको निर्देशन बमोजिम प्राप्त गरेको जानकारीका सम्बन्धमा तत्कालै केन्द्रलाई जानकारी गराउनु पर्नेछ ।

(४) उपदफा (१) बमोजिम खटिएको व्यक्तिले उचित र पर्याप्त कारण वेगर केन्द्रलाई जानकारी नगराएमा विभागीय सजाय हुनेछ ।

(५) कुनै पनि व्यक्तिले उचित र पर्याप्त कारण वेगर उपदफा (१) बमोजिमका उपाय अवलम्बन गर्न वा अन्य कुनै शर्त पालना गर्न अवरोध गर्नु वा दिईएको निर्देशनको अवज्ञा गर्नु हुँदैन ।

(६) सम्बन्धित व्यक्तिले लिखित मन्जुरी दिएमा बाहेक अन्य अवस्थामा यस दफा बमोजिम सङ्कलन गरिएका जानकारीहरु कानून कार्यान्वयन गर्ने निकायमा पेश गर्ने बाहेक अन्य अवस्थामा सार्वजनिक गर्नु हुँदैन ।

(७) उपदफा (६) विपरित कार्य गर्ने व्यक्तिलाई विभागीय सजाय हुनेछ ।

परिच्छेद- ७

साईबर सुरक्षा सेवा प्रदायक अनुमतिपत्र सम्बन्धी व्यवस्था

२७. **अनुमतिपत्र प्राप्त व्यक्ति बाहेक अरुले साईबर सुरक्षा सम्बन्धी सेवा प्रदान गर्न नहुने:** कसैले पनि दफा २८ बमोजिम जारी गरिने साईबर सुरक्षा सेवा प्रदायकको अनुमतिपत्र प्राप्त नगरी अनुसूची- २ मा उल्लिखित साईबर सुरक्षा सेवा प्रदान गर्न पाउने छैन ।

२८. **अनुमतिपत्र सम्बन्धी व्यवस्था**: (१) केन्द्रले साईबर सुरक्षा सेवा प्रदायकको अनुमतिपत्र जारी गर्न सक्नेछ ।

(२) साईबर सुरक्षा सेवा प्रदायकको अनुमतिपत्र प्राप्त गर्न आवश्यक पर्ने शैक्षिक योग्यता, अनुमतिपत्र दस्तुर, अनुमतिपत्र प्राप्त गर्न लिईने परीक्षा, अनुमतिपत्र नविकरण दस्तुर र अन्य कुरा तोकिए बमोजिम हुनेछन् ।

२९. **अनुमतिपत्र तथा अनुमतिपत्रको नविकरण**: (१) साईबर सुरक्षा प्रदान गर्न पाउने अनुमतिपत्र प्राप्त गर्न चाहने व्यक्तिले तोकिए बमोजिमको शुल्क र अन्य आवश्यक कुरा समावेश गरी केन्द्र समक्ष निवेदन दिनु पर्नेछ ।

(२) अनुमतिपत्र प्राप्त व्यक्तिले अनुमतिपत्रको अवधी समाप्त हुनु एक महिना अघि अनुमतिपत्र नविकरण गर्न आवश्यक दस्तुर समावेश गरी केन्द्र समक्ष निवेदन दिनु पर्नेछ ।

(३) केन्द्रले उपदफा (१) वा (२) बमोजिम निवेदन प्राप्त गरेमा आवश्यक छानविन गरी अनुमतिपत्र प्रदान गर्न वा नविकरण गर्न सक्नेछ ।

(४) अनुमतिपत्र प्राप्त गर्न चाहने कुनै व्यक्तिले झुट्टा विवरण पेश गर्नु हुँदैन ।

३०. **अनुमतिपत्रका शर्तहरु**: (१) केन्द्रले आवश्यक शर्त तोकि अनुमतिपत्र प्रदान गर्न सक्नेछ ।

(२) उपदफा (१) को प्रयोजनको लागि केन्द्रले देहायका कुरा तोक्न सक्नेछः-

(क) अनुमतिपत्र प्राप्त गर्ने व्यक्तिले पालना गर्नु पर्ने शर्तहरु,

(ख) कुनै खास वर्गमा पर्ने अनुमतिपत्र प्राप्त गर्ने व्यक्तिले पालना गर्नु पर्ने शर्तहरु ।

(३) केन्द्रले उपदफा (१) बमोजिम तोकेका शर्तहरु आवश्यकता अनुसार थपघट वा हेरफेर सक्नेछ ।

३१. **अनुमतिपत्रको ढाँचा तथा अवधि**: (१) अनुमतिपत्रको ढाँचा तोकिए बमोजिम हुनेछ र यसमा अनुमतिपत्र जारी गरिने शर्तहरु रहने छन् ।

(२) अनुमतिपत्रको अवधि अनुमतिपत्र जारी गरेको मितिले पाँच वर्षको हुनेछ ।

(३) नविकरण गरिएको अनुमतिपत्रको अवधि समेत अनुमतिपत्र नविकरण गरिएको मितिले पाँच वर्षको हुनेछ ।

३२. **अभिलेख राख्नु पर्ने**: (१) अनुमतिपत्र प्राप्त व्यक्तिले साईवर सुरक्षा सेवा प्रदान गर्दा पटकै पिच्छे देहायका विवरण सहित अभिलेख राख्नु पर्नेछः

(क) अनुमतिपत्र प्राप्त व्यक्तिलाई साईबर सुरक्षा सेवामा लगाउने व्यक्तिको नाम तथा ठेगाना,

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

(ग) साईबर सुरक्षा सेवा प्रदान गरिएको मिति,

(घ) कस्तो सेवा प्रदान गरिएको हो सो को विवरण,

(ङ) तोकिए बमोजिमका अन्य विवरणहरु ।

(२) अनुमतिपत्र प्राप्त व्यक्तिले साईवर सुरक्षा सेवा प्रदान गरेको पटकै पिच्छे उपदफा (१) बमोजिमको विवरण सहितको अभिलेख केन्द्रलाई उपलब्ध गराउनु पर्नेछ र त्यस्तो अभिलेख तीन वर्ष सम्म सुरक्षित राख्नु पर्नेछ ।

(१) उपदफा (१) बमोजिमको अभिलेख बुझाउने ढाँचा तोकिए बमोजिम हुनेछ ।

(३) प्रत्येक अनुमतिपत्र प्राप्त व्यक्तिले तोकिएको ढाँचा तथा समय भित्र केन्द्रलाई अभिलेख बुझाउनु पर्नेछ । कसैले जानी जानी गलत सूचना दिनु वा अभिलेखमा रहेको कुनै कुरा हटाउनु हुँदैन ।

३३. **अनुमतिपत्रको खारेज वा निलम्बन गर्न सक्ने**: अनुमतिपत्र प्राप्त व्यक्तिले देहायको काम कुरा गरेको छ भन्ने कुरामा केन्द्र विश्वस्त भएमा उपदफा (४) को अधिनमा रही केन्द्रले अनुमतिपत्र खारेज वा निलम्बन गर्न सक्नेछः-

(क) अनुमतिपत्र प्राप्त व्यक्तिले अनुमतिपत्रका शर्तहरु पालना नगरेमा,

(ख) झुट्टा विवरण दिई अनुमतिपत्र प्राप्त गरेको भएमा,

(ग) अनुमतिपत्र प्राप्त व्यक्तिले जुन प्रयोजनको लागि अनुमतिपत्र दिईएको हो सोसँग सम्बन्धित व्यापार व्यवसाय नेपाल भित्र संचालन गरेमा,

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

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

(२) अनुमपतपत्र खारेज गर्ने पर्याप्त कारण नभएमा केन्द्रले देहाय बमोजिम गर्न सक्नेछः-

(क) छ महिना अवधि ननाघ्ने गरी अनुमतिपत्र निलम्बन गर्ने,

(ख) सम्बन्धित अनुमतिपत्र प्राप्त व्यक्तिलाई चेतावनी दिने,

(ग) केन्द्रले उपयुक्त देखेको अन्य शर्त थप्ने ।

(३) कारबाही गर्न लागिएको सम्बन्धित अनुमतिपत्र प्राप्त व्यक्तिलाई सफाई पेश गर्ने मनासिव मौका नदिई कारबाही गर्नु हुँदैन र त्यस्तो सफाई पेश गर्न दुई हप्ताको समय दिनु पर्नेछ ।

(४) अनुमतिपत्र खारेज गर्न वा निलम्बन गर्न सूचना दिएपछि सम्बन्धित अनुमतिपत्र प्राप्त व्यक्तिको अनुमतिपत्र खारेज वा निलम्बन हुनेछ ।

परिच्छेद- ७

अनुसन्धान तथा प्रमाण सम्बन्धी व्यवस्था

३४. **अनुसन्धान अधिकृत**: यस ऐन बमोजिमको कसूर सम्बन्धी मुद्दाको अनुसन्धान साईवर सुरक्षा सम्बन्धी ज्ञान भएको कम्तिमा प्रहरी निरीक्षक दर्जाको अधिकृतले गर्नेछ ।

३५. **खानतलासी गरी कब्जामा लिन सक्ने:** (१) अनुसन्धान अधिकृतले कुनै कसूर प्रमाणित गर्ने प्रमाणमा लाग्न सक्ने कम्प्युटर वा कम्प्युटर प्रणाली वा अन्य त्यस्तै वस्तु रहेको स्थानमा प्रवेश गरी खानतलासी लिन, कम्प्युटर वा कम्प्युटर प्रणाली, कागजात वा त्यस्तै अन्य कुनै वस्तु कब्जामा लिन सक्नेछ ।

(२) उपदफा (१) बमोजिमको खानतलासी तथा कुनै माल वस्तु कब्जामा लिनु परेमा अनुसन्धान अधिकृतले त्यस्तो खानतलासी तथा कब्जा गर्न आवश्यक रहेको पुष्टि गर्ने तत्काल प्राप्त प्रमाण वा विश्वसनीय आधार भएमा त्यस्ता प्रमाण वा आधार सहित अदालत समक्ष निवेदन दिनु पर्नेछ ।

(३) उपदफा (१) बमोजिमको निवेदनसाथ प्राप्त प्रमाण वा आधारमा अदालत सन्तुष्ट भएमा उपदफा (१) बमोजिमको खानतलासि तथा कब्जाको लागि अनुसन्धान अधिकृतलाई अनुमती दिन सक्नेछ ।

(४) अनुसन्धान अधिकृतले दफा (१) बमोजिम खानतलासी वा कब्जा गर्दा देहाय बमोजिमको कार्य तुरुन्त गर्नु पर्नेछ:-

(क) जफत गरेको मिति र समय खुलाई कब्जामा लिएका वस्तुहरुको सूची तयार गर्ने,

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

(ग) खानतलासि गरिएको स्थान नियन्त्रणमा राख्ने,

(घ) कब्जामा लिएका वस्तुहरुको संरक्षणको प्रत्याभूति गर्ने ।

(५) उपदफा (१) बमोजिम खानतलासी लिने अनुसन्धान अधिकृतलाई खानतलास गरी प्राप्त गर्न खोजिएको कुरा अर्को कुनै विद्युतीय प्रणालीमा रहेको वा त्यस्तो प्रणालीको कुनै अंश क्षेत्राधिकार भित्रै रहेको अर्को कुनै प्रणालीमा रहेको वा त्यस्तो सूचना प्रारम्भिक प्रणालीबाट कानून बमोजिम पहुँच राख्न सकिने अर्को प्रणालीमा रहेको छ भन्ने लागेमा निजले तत्कालै त्यस्तो खानतलासी विस्तार गरी त्यस्तो प्रणालीमा पहुँच राख्न सक्नेछ ।

३६. **आवश्यक सहयोग गर्नु पर्ने**: अनुसन्धान अधिकृतले खानतलासीको क्रममा कुनै कम्प्युटर वा कम्प्युटर प्रणाली अभियोग पत्रमा नाम समावेश नभएको कुनै व्यक्तिको कब्जा वा नियन्त्रणमा रहेको पाएमा त्यस्तो व्यक्तिले अनुसन्धान अधिकृतलाई कम्प्युटर वा कम्प्युटर प्रणालीसम्म

पहुँच राख्न वा प्रयोग गर्न वा प्रतिलिपि उतार गर्न, ईन्क्रिप्ट गरिएको सूचनालाई डिक्रिप्ट गर्न अनुमति दिई अन्य आवश्यक सहयोग गर्नु पर्नेछ ।

३७. **झिकाउने आदेश दिन सक्ने**: (१) कुनै कसूरको अनुसन्धान वा अभियोजन प्रयोजनको लागि कुनै खास कम्प्युटर वा कम्प्युटर प्रणाली आवश्यक रहेको कुरामा अदालत समक्ष पेश भएको प्रमाणको आधारमा अदालत सन्तुष्ट भएमा त्यस्तो कम्प्युटर वा कम्प्युटर प्रणाली नियन्त्रणमा राख्ने व्यक्तिलाई उक्त कम्प्युटर वा कम्प्युटर प्रणाली पेश गर्न आदेश गर्न सक्नेछ ।

(२) उपदफा (१) बमोजिमको कम्प्युटर वा कम्प्युटर प्रणाली अदालत समक्ष पेश गर्नु सम्बन्धित व्यक्तिको कर्तव्य हुनेछ ।

३८. **तत्काल संरक्षण गर्नु पर्ने**: केन्द्रले साईबर सुरक्षा जोखिम रहेको वा घटना भएको कुनै कम्प्युटर वा कम्प्युटर प्रणालीलाई तत्कालै संरक्षण गर्नु पर्नेछ ।

परिच्छेद- ८

कसूर सजाय

३९. **कसूर गरेको मानिने**: (१) कसैले देहायको कुनै कार्य गरे गराएमा यस ऐन अन्तर्गतको कसूर गरेको मानिनेछ:-

(क) दफा १५ को उपदफा (१) विपरितको कार्य,

(ख) दफा १७ को उपदफा (१) विपरितको कार्य,

(ग) दफा १९ विपरितको कार्य,

(घ) दफा २० को उपदफा (१) विपरितको कार्य,

(ङ) दफा २१ को उपदफा (१) र (७) विपरितको कार्य,

(च) दफा २२ को उपदफा (५) विपरितको कार्य,

(छ) दफा २३ को उपदफा (६) विपरितको कार्य,

(छ) दफा २६ को उपदफा (५) विपरितको कार्य,

(ज) दफा २७ विपरितको कार्य,

(झ) दफा २९ को उपदफा (४) विपरितको कार्य,

(ञ) दफा ३२ को उपदफा (३) विपरितको कार्य,

४०. **सजाय**: दफा ३९ बमोजिमको कसूरमा देहाय बमोजिमको सजाय हुनेछ:-

(क) दफा १५ को उपदफा (१) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी दुईलाख रुपैयाँसम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(ख) दफा १७ को उपदफा (१) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी दुईलाख रुपैयाँसम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(ग) दफा १७ को उपदफा (३) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी एकलाख रुपैयाँसम्म जरिवाना वा एक वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(घ) दफा १९ को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी दुईलाख रुपैयाँसम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(ङ) दफा २१ को उपदफा (१) र (७) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी दुईलाख रुपैयाँसम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(च) दफा २२ को उपदफा (५) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी एक लाख रुपैयाँसम्म जरिवाना वा एक वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(छ) दफा २३ को उपदफा (६) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी एक लाख रुपैयाँसम्म जरिवाना वा एक वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(ज) दफा २६ को उपदफा (५) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी पाँलाख रुपैयाँसम्म जरिवाना वा पाँच वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(झ) दफा २७ को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी दुईलाख रुपैयाँसम्म जरिवाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(ञ) दफा २९ को उपदफा (४) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी एकलाख रुपैयाँसम्म जरिवाना वा एक वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

(ट) दफा ३२ को उपदफा (३) को कसूरमा कसूरदारलाई कसूरको मात्रा हेरी एकलाख रुपैयाँसम्म जरिवाना वा एक वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

४१. **कसूर गर्न दुरुत्साहन गर्न नहुने**: कसैले यस ऐन बमोजिमको कुनै कसूर गर्न कसैलाई दुरुत्साहन गरेमा वा त्यस्तो कसूर गर्न उद्योग गरेमा वा षडयन्त्रमा संलग्न भएमा त्यस्तो व्यक्तिलाई मुख्य कसूरदारलाई भए सरहको सजाय हुनेछ ।

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

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

४४. **प्रचलित कानून बमोजिम सजाय गर्न बाधा नपर्ने**: 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 ।

तर एकै कसूरमा एक भन्दा बढी सजाय हुने छैन ।

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

४६. **नेपाल सरकार वादी हुने**: (१) यस ऐन बमोजिमको कसूरसँग सम्बन्धित मुद्दामा नेपाल सरकार वादी हुनेछ ।

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

४७. **मुद्दा हेर्ने अधिकारी**: यस ऐन बमोजिमको कसूरसँग सम्बन्धित मुद्दाको कारबाही र किनारा गर्ने अधिकार नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकेको अदालतलाई हुनेछ ।

४८. **पुनरावेदन लाग्न सक्ने**: (१) दफा ४७ बमोजिमको अदालतले गरेको निर्णय वा अन्तिम आदेश उपर चित्त नबुझ्ने पक्षले त्यस्तो आदेश वा निर्णय भएको मितिले नव्वे दिनभित्र सम्बन्धित उच्च अदालत समक्ष पुनरावेदन दिन सक्नेछ ।

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

परिच्छेद- ९

प्रमुख कार्यकारी अधिकृत र कर्मचारी सम्बन्धी व्यवस्था

४९. **प्रमुख कार्यकारी अधिकृत**: (१) नेपाल सरकारले केन्द्रको प्रमुख भई काम गर्न नेपाल सरकारको विशिष्ट श्रेणी वा राजपत्राङ्कित प्रथम श्रेणी वा सो सरहको पदमा रही काम गरिसकेको वा ईन्जिनियरिङ्ग, विज्ञान, कानून, सूचना प्रविधि, मानविकि वा व्यवस्थापन विषयमा कम्तिमा स्नाकोत्तर उपाधि हासिल गरी सूचना प्रविधिको क्षेत्रमा व्यवस्थापकीय जिम्मेवारी लिई कम्तिमा पन्ध्र वर्षको अनुभव प्राप्त गरेको व्यक्तिहरुमध्येबाट प्रमुख कार्यकारी अधिकृतको पदमा नियुक्ति गर्न सक्नेछ ।

(२) उपदफा (१) बमोजिमको योग्यता भएको व्यक्तिहरु मध्येबाट प्रमुख कार्यकारी अधिकृतको पदमा नियुक्ति गर्नको लागि मन्त्रालयले सार्वजनिक रुपमा दरखास्त आव्हान गर्नु पर्नेछ ।

(३) प्रमुख कार्यकारी अधिकृतको सिफारिस गर्न लोकसेवा आयोगको सदस्यको अध्यक्षतामा देहाय बमोजिमको एक सिफारिस समिति रहनेछः-

(क) लोक सेवा आयोगको सदस्य -अध्यक्ष

(ख) सचिव, मन्त्रालय -सदस्य

(ग) मन्त्रालयले तोकेको एकजना विषय विज्ञ - सदस्य

(घ) सह सचिव, मन्त्रालय -सदस्य सचिव

(४) उपदफा (३) बमोजिमको सिफारिस समितिले तोकिएको आधारमा खुल्ला प्रतियोगिताद्वारा सबैभन्दा बढी अङ्क प्राप्त गर्ने उम्मेदवारलाई नियुक्तिको लागि नेपाल सरकार समक्ष सिफारिस गर्नेछ ।

(५) उपदफा (४) बमोजिम सिफारिस गरिएको व्यक्तिलाई नेपाल सरकारले प्रमुख कार्यकारी अधिकृतको पदमा नियुक्ति गर्नेछ ।

(६) उपदफा (५) बमोजिम प्रमुख कार्यकारी अधिकृतको नियुक्ति नभएसम्मको लागि कम्तिमा निजामती सेवाको राजपत्राङ्कित प्रथम श्रेणी वा सो सरहको पदमा कार्यरत कुनै अधिकृतलाई नेपाल सरकारले प्रमुख कार्यकारी अधिकृतको पदमा काम काज गर्ने गरी खटाउन सक्नेछ ।

(७) प्रमुख कार्यकारी अधिकृतको पदावधि चार वर्षको हुनेछ ।

(८) उपदफा (६) मा जुनसुकै कुरा लेखिएको भएता पनि देहायको अवस्थामा नेपाल सरकारले प्रमुख कार्यकारी अधिकृतलाई पदबाट हटाउन सक्नेछः-

(क) यो ऐन र यस ऐन अन्तर्गत बनेको नियमावली बमोजिम सम्पादन गर्नु पर्ने काम कार्यान्वयन गर्न वा गराउन निजमा कार्यक्षमताको अभाव भएमा,

(ख) निजले केन्द्रको नीति विपरित कुनै काम कारबाही गरेमा,

(ग) निजको आचरण खराव भएमा,

(घ) निजले सम्पादन गरेको कार्यको कार्य सम्पादनस्तर सत्तरी प्रतिशत भन्दा कम भएमा ।

(९) उपदफा (८) बमोजिम पदबाट हटाउनु अघि निजलाई आफ्नो सफाई पेश गर्ने मनासिव मौका दिनु पर्नेछ ।

(१०) प्रमुख कार्यकारी अधिकृतले तोकिए बमोजिमको ढाँचामा स्वार्थ नबाझिएको घोषणा गर्नु पर्नेछ ।

(११) प्रमुख कार्यकारी अधिकृतको नियुक्तिको सिफारिस गर्ने अन्य प्रक्रिया तथा बैठक सम्बन्धी अन्य कार्यविधि उपदफा (३) बमोजिमको सिफारिस समितिले निर्धारण गरे बमोजिम हुनेछ ।

५०. **प्रमुख कार्यकारी अधिकृत पदको लागि अयोग्यता**: देहायको व्यक्ति प्रमुख कार्यकारी अधिकृतको पदमा नियुक्ति हुन वा वहाल रहन योग्य मानिने छैनः-

(क) गैरनेपाली नागरिक,

(ख) ४० वर्ष पूरा नभएको र ६० वर्ष नाघेको,

(ग) विदेशी मुलुकको स्थायी आवासीय अनुमतिपत्र लिएको,

(घ) भ्रष्टाचार, जबरजस्ति करणी, मानव बेचबिखन तथा ओसारपसार, लागू औषध कारोबार, सम्पत्ति शुद्धिकरण, वन्यजन्तुको ओसारपसार, संगठीत अपराध, राहदानी दुरुपयोग, अपहरण सम्बन्धी कसूर वा नैतिक पतन देखिने फौजदारी कसूरमा अदालतबाट सजाय पाएको,

(ङ) प्रचलित कानून बमोजिम कालो सूचीमा परेको वा त्यस्तो सूचीबाट फुकुवा भएको तीन वर्ष पूरा नभएको,

(च) कुनै राजनैतिक दलको सदस्य वा पदाधिकारी भएको ।

५१. **प्रमुख कार्यकारी अधिकृतको काम, कर्तव्य र अधिकार**: यस ऐनमा अन्यत्र लेखिएको काम कर्तव्य र अधिकारको अतिरिक्त प्रमुख कार्यकारी अधिकृतको काम, कर्तव्य र अधिकार देहाय बमोजिम हुनेछः-

(क) समितिको निर्णय कार्यान्वयन गर्ने गराउने,

(ख) केन्द्रको वार्षिक कार्यक्रम तयार गरी समिति समक्ष पेश गर्ने,

(ग) केन्द्रबाट भए गरेका कामको प्रगति विवरण अध्यावधिक रुपमा समिति समक्ष पेश गर्ने,

(घ) केन्द्रको प्रमुखको हैसियतले दैनिक प्रशासनिक कार्य संचालन र व्यवस्थापन गर्ने तथा मातहतका कर्मचारीको रेखदेख, नियन्त्रण, निर्देशन, अनुगमन, मूल्याङ्कन र सुपरीवेक्षण गर्ने,

(ङ) समितिबाट स्वीकृत हुनु पर्ने प्रस्तावहरु समिति समक्ष पेश गर्ने,

(च) केन्द्रको काम, कारबाहीका सम्बन्धमा विभिन्न निकायहरु बीच समन्वय र सहकार्य गर्ने,

(छ) समितिले गर्ने भनिएका काम बाहेक केन्द्रले गर्ने सम्पूण कार्य गर्ने,

(ज) तोकिए बमोजिमका अन्य कार्य गर्ने ।

५२. **कार्यसम्पादन सम्झौता गर्नु पर्ने**: (१) दफा ४९ बमोजिम नियुक्त प्रमुख कार्यकारी अधिकृतले मन्त्रालयसँग कार्य सम्पादन सम्झौता गर्नु पर्नेछ ।

(२) उपदफा (१) बमोजिम गरिने कार्यसम्पादन समझौतामा प्रमुख कार्यकारी अधिकृतले सम्पादन गर्नु पर्ने कार्य, सोको कार्ययोजना, सम्पादन हुने कामको मूल्याङ्कनका सूचक आदि उल्लेख गर्नु पर्नेछ ।

(३) प्रमुख कार्यकारी अधिकृतले एक वर्षभरी आफूले सम्पादन गरेको कामको वार्षिक प्रतिवेदन प्रत्येक आर्थिक वर्ष समाप्त भएको ६० निदभित्र मन्त्रालय समक्ष पेश गर्नु पर्नेछ ।

५३. **प्रमुख कार्यकारी अधिकृतको पारिश्रमिक**: प्रमुख कार्यकारी अधिकृतको पारिश्रमिक नेपाल सरकारले तोके बमोजिम हुनेछ ।

५४. **कर्मचारी सम्बन्धी व्यवस्था**: (१) केन्द्रमा आवश्यक संख्यामा कर्मचारीहरु रहनेछन् ।

(२) उपदफा (१) बमोजिमका कर्मचारीको नियुक्ति, पारिश्रमिक, सुविधा तथा सेवाका अन्य शर्तहरु कमर्मचारी सम्बन्धी विनियमावली बमोजिम हुनेछ ।

(३) केन्द्रले आवश्यकता अनुसार अवधि तोकी विशेषज्ञ सेवा करारमा लिन सक्नेछ ।

(४) उपदफा (३) बमोजिम करारमा लिईएका विशेषज्ञको सेवाको शर्त, पारिश्रमिक र अन्य कुरा करारमा उल्लेख भए बमोजिम हुनेछ ।

(५) यस ऐन बमोजिमका कमर्मचारी नियुक्ति नभएसम्मको लागि केन्द्रको सिफारिसमा मन्त्रालयले नेपाल सरकार वा नेपाल सरकारको स्वामित्वमा रहेको संगठीत संस्थाका कर्मचारीलाई काजमा तोकिए बमोजिम खटाउन सक्नेछ ।

परिच्छेद- १०

विविध

५५. **नेपाल सरकारले निर्देशन दिन सक्ने**: यो ऐन कार्यान्वयन गर्ने सम्बन्धमा नेपाल सरकारले नेपाल सरकारका निकायहरुलाई आवश्यक निर्देशन दिन सक्नेछ र त्यस्तो निर्देशनको पालना गर्नु त्यस्ता सबै निकायको कर्तव्य हुनेछ ।

५६. **उजुर गर्ने हदम्याद**: यो ऐन वा यो ऐन अन्तर्गत बनेको नियमको उल्लंघन भएकोमा वा यो ऐन बमोजिम कसूर ठहर्ने कुनै कुरा भएकोमा त्यस्तो उल्लंघन वा कसूर भए गरेको थाहा पाएको मितिले तीन महिना भित्र उजुर गर्नु पर्नेछ ।

५७. **बाधा अडकाउ फुकाउने अधिकार**: यो ऐन कार्यान्वयन गर्न कुनै बाधा अडकाउ परेमा नेपाल सरकारले त्यस्तो बाधा अडकाउ फुकाउनको लागि नेपाल राजपत्रमा सूचना प्रकाशन गरी सूचना जारी गर्न सक्नेछ ।

५८. **नियम बनाउने अधिकार**: (१) यो ऐनको उद्देश्य कार्यान्वयन गर्न नेपाल सरकारले देहायका विषयहरुमा आवश्यक नियमहरु बनाउन सक्नेछ:-

(क) संवेदनशील सूचना पूर्वाधार तोक्ने कार्यविधि सम्बन्धमा,

(ख) संवेदनशील सूचना पूर्वाधार सम्बन्धमा पालना गर्नु पर्ने प्राविधिक वा अन्य मापदण्डहरु निर्धारण गर्ने सम्बन्धमा,

(ग) संवेदनशील सूचना पूर्वाधारका धनीको जिम्मेवारी तथा कर्तव्य सम्बन्धमा,

(घ) संवेदनशील सूचना पूर्वाधारको डिजाईन, कन्फिगुरेसन, सुरक्षा वा संचालनमा गरिएको तात्विक परिवर्तन र सो सम्बन्धी जानकारी दिनु पर्ने तरिकाका सम्बन्धमा,

(ङ) संवेदनशील सूचना पूर्वाधार सम्बन्धी के कस्ता घटनाको जानकारी दिनु पर्ने भन्ने सम्बन्धमा,

(च) संवेदनशील सूचना पूर्वाधारको साईवर सुरक्षा सम्बन्धी अडिट गराउनु पर्ने विषयका सम्बन्धमा,

(छ) साईबर सुरक्षाका गरिने कारबाहीको स्वरुप र प्रकृतिका सम्बन्धमा,

(ज) जारी गरिने अनुमतिपत्रको वर्ग, अनुमतिपत्र प्राप्त गर्न चाहिने योग्यता र अनुमतिपत्रको नविकरण सम्बन्धमा,

(झ) अनुमतिपत्र प्रदान गर्न सञ्चालन गरिने परीक्षा, दस्तुर तथा सोसँग सम्बन्धित अन्य कुराका सम्बन्धमा ।

५९. **अनुसूचीमा हेरफेर गर्न सक्ने**: नेपाल सरकारले समय समयमा नेपाल साजपत्रमा सूचना प्रकाशन गरी अनुसूचीमा हेरफेर गर्न सक्नेछ ।

६०. **नेपाल सरकारसँग सम्पर्क**: केन्द्रले नेपाल सरकारसँग सम्पर्क गर्दा सूचना प्रविधि तथा संचार मन्त्रालय मार्फत गर्नु पर्नेछ ।

६१. विनियम तथा **निर्देशिका बनाई लागू गर्न सक्ने**: यस ऐनको उद्देश्य पूर्ति गर्नको लागि केन्द्रले यो ऐन वा यो ऐन अन्तर्गत बनेका नियमहरुको अधीनमा रही आवश्यक विनियम, निर्देशिका तथा मापदण्ड बनाई लागू गर्न सक्नेछ ।

अनुसूची- १

(दफा २ को खण्ड (क) सँग सम्बन्धित)

१. **उर्जासँग सम्बन्धित सेवाहरु**

(क) विद्युत उत्पादन, प्रशारण र वितरण सेवाहरु

२. **सूचना-संचार सम्बन्धित सेवाहरु**

(क) स्थिर टेलिफोन सेवाहरु

(ख) मोवाईल टेलिफोन सेवाहरु

(ग) बोर्डव्याण्ड ईन्टरनेट पहुँच सेवाहरु

(घ) राष्ट्रिय डोमेन नाम दर्ता सेवाहरु

३. **खानेपानीसँग सम्बन्धित सेवाह**रु

(क) खानेपानी वितरण सेवा

४. **स्वास्थ्य हेरचाहसँग सम्बन्धित सेवाहरु**

(क) आकस्मिक हस्पिटल हेरचाह सेवा

(ख) रोग निगरानी तथा अनुक्रिया सेवाहरु

५. **बैङ्क तथा फाईनान्ससँग सम्बन्धित सेवाहरु**

(क) नगद झिक्ने तथा जम्मा गर्ने, संस्थागत ऋण प्रवाह, कोष व्यवस्थापन तथा भुक्तानी सेवाहरु समेतका बैङ्किग सेवाहरु

(ख) भुक्तानी राफसाफ सेवाहरु, भुक्तानी समासोधन तथा भुक्तानी प्रणाली सम्बन्धी सेवाहरु

(ग) धितोपत्र व्यापार, राफसाफ, भुक्तानी तथा जम्मा गर्ने सम्बन्धी सेवाहरु

(घ) मौद्रिक तथा फाईनान्सियल स्थायित्व कायम गर्ने सम्बन्धी सेवाहरु

(ङ) मुद्रा निष्काशन

(च) नगद व्यवस्थापन तथा सरकारलाई गरिने भुक्तानी सम्बन्धी सेवाहरु

६. **सुरक्षा तथा आपतकालसँग सम्बन्धित सेवाहरु**

(क) नागरिक सुरक्षा सेवाहरु

(ख) प्रहरी तथा सुरक्षा सेवाहरु

(ग) अध्यागमन सेवाहरु

(घ) कारागार पुनर्स्थापन तथा पुनर्स्थापना सम्बन्धी सेवाहरु

७. **नागरिक उड्डयनसँग सम्बन्धित सेवाहरु**

(क) हवाई उडान सम्बन्धी सेवाहरु

(ख) हवाई यात्रु नियन्त्रण तथा संचालन

(ग) हवाई व्यागेज तथा कार्गो संचालन

(घ) हवाई जहाज मैदान संचालन

(ङ) हवाई जहाज उड्डयन संचालन

८. **सरकार संचालनसँग सम्बन्धित सेवाहरु**

(क) सरकारद्वारा सर्वसाधारणलाई विद्युतीय सार्वजनिक सेवा उपलव्ध गराउने सम्बन्धी सेवाहरु

(ख) सरकारका आन्तरिक काम कारबाही विद्युतीय माध्यमबाट प्रशोधन गर्ने

९. **संचार माध्यमसँग सम्बन्धित सेवाहरु**

(क) टेलिभिजन तथा रेडियो प्रशारण सम्बन्धी सेवाहरु

(ख) अखवार छपाई सम्बन्धी सेवाहरु

(ग) सुरक्षण मुद्रण समबन्धी सेवाहरु

१०. **अन्य**

क. सूचना भण्डारण केन्द्र सम्बन्धी

ख. डिजिटल सूचना भण्डारण सम्बन्धी

अनुसूची- २

(दफा २ को खण्ड (घ), (प) र २७ सँग सम्बन्धित)

अनुमतिपत्र आवश्यक पर्ने साईवर सुरक्षा सेवाहरु

१. अर्को व्यक्तिको कम्प्युटर वा कम्प्युटर प्रणालीको साईवर सुरक्षा जोखिमको स्तर पत्ता लगाउने प्रयोजनको लागि त्यस्तो कम्प्युटर वा कम्प्युटर प्रणालीमा भण्डारण गरिएको, प्रशोधन गरिएको वा प्रशारण गरिएको कुरा प्राप्त, पहिचान, वा स्क्यान गरी अनुगमन गर्ने सेवा ।

२. कुनै कम्प्युटर वा कम्प्युटर प्रणालीको साईवर सुरक्षा कमजोरी निर्धारण, परीक्षण वा मूल्याङ्कन गर्न प्रदान गरिने अडिटिङ सेवा ।