एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र
(Integrated Anti-Cyber Scam Center - IACSC)
स्थापना र कार्यसञ्चालन सम्बन्धी दिग्दर्शन-२०८३

नेपाल सरकार
गृह मन्त्रालय
२०८३

गोविन्दनाथ शर्मा
सचिव

एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र (Integrated Anti-Cyber Scam Center - IACSC) को स्थापना र कार्य सञ्चालन सम्बन्धी दिग्दर्शन-२०८३

मन्त्रालयबाट स्वीकृत मिति २०८३/६/२३ गते

प्रस्तावना :

विद्युतीय माध्यमको दुरुपयोग गरी हुने गरेका ठगी, साइबर स्क्यामको प्रभावकारी रोकथाम र अनुसन्धान गरी राज्यको वित्तीय क्षेत्र सुरक्षित र विश्वसनीय बनाउने तथा आम नागरिकलाई साइबर स्क्याम, ठगी हुनबाट बचाउनको लागि नियामक निकाय नेपाल राष्ट्र बैंक, नेपाल दुरसञ्चार प्राधिकरण, बैंक तथा वित्तीय संस्था, भुक्तानी सेवा प्रदायक, भुक्तानी प्रणाली सञ्चालक, दूरसञ्चार सेवा प्रदायक संस्थाहरू र कानून कार्यान्वयन निकायको संयुक्त सहभागितामा चौविसै घण्टा सञ्चालन हुने गरी उल्लिखित निकायहरुसँगको परामर्श तथा राय/सहमति बमोजिम एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रको (IACSC) स्थापना गर्न वाञ्छनीय भएकोले सुशासन व्यवस्थापन तथा सञ्चालन ऐन २०६४ को दफा ४५ ले दिएको अधिकार प्रयोग गरी यो दिग्दर्शन तयार गरिएको छ।

१. पृष्ठभूमि (Background):

डिजिटल बैंकिङ, इ-वालेट, अनलाइन भुक्तानी प्रणाली र सामाजिक सञ्जालको वृद्धिसंगै साइबर स्क्याम, ठगी र वित्तीय कसुरका घटनाहरूमा भएको तीव्र बढोत्तरीले डिजिटल वित्तीय प्रणालीको विश्वसनीयतामा गम्भीर चुनौती सिर्जना भएको छ । विगतमा व्यक्तिगत स्तरमा देखिएका साइबर स्क्याम हालका दिनमा अन्तरदेशीय संगठित आपराधिक समूहमार्फत सञ्चालित हुने गरेका छन् । जसमा स्वदेश तथा विदेशमा अवैध रूपमा स्थापना गरेका स्क्याम कल सेन्टरहरूले नेपाली बैंक खाता तथा इ-वालेटलाई लक्षित गरी स्क्याम गर्ने र मनी म्युलहरूलाई प्रयोग गरी विभिन्न खातामा लेयरिङ गरी/गराई अवैध रेमिट्यान्स (हुण्डी) बाट प्राप्त हुनुपर्ने रकम वा अन्य प्रयोजनका लागि प्राप्त हुनुपर्ने रकम वापत समेत स्क्याम भएको रकमलाई रकमान्तर गराई वा नगद निकाली (Cash-out) आर्थिक लाभ लिने प्रवृत्ति बढ्दै गएको छ।

डिजिटल भुक्तानी प्रणाली र इन्टरनेट बैंकिङ सेवाको विस्तारसँगै नेपालको अर्थतन्त्र र नागरिकको दैनिक जीवन डिजिटल पूर्वाधारमा निर्भर हुँदै गएको छ । यस सहजताको दुरुपयोग गर्दै संगठित आपराधिक सञ्जालले डिजिटल माध्यमबाट हुने स्क्यामलाई एक सुनियोजित व्यवसायको रूपमा विकास गरेको देखिन्छ। यसको कारण साइवर स्क्याम, ठगीहरू मध्ये Investment Related Scam, Online Job Scam, Romance Scam, Online Marketplace Related Scam, Digital Arrest/Blackmailing, QR/Wallet Scam, Malicious Link/File, Cryptocurrency Related Scam, Sim Swap, Social Engineering Scam (Phishing, Smishing, Vishing), Lottery/Gift/Parcel, Online Betting जस्ता समस्याहरु वर्तमान अवस्थामा साइबर तथा वित्तीय सुरक्षा कायम गर्नका लागि प्रमुख चुनौतीको रुपमा विकास भएका छन्।

डिजिटल भुक्तानी प्रणालीको पहुँचको विस्तार गर्नु नेपाल सरकारको प्राथमिकतामा रहेको विद्यमान अवस्थामा साइबर स्क्याम गर्ने गिरोहहरूले वित्तीय असाक्षरताको फाइदा उठाउँदै बेरोजगार युवा-युवती तथा वृद्ध-वृद्धाहरूलाई विभिन्न बहानामा बैंक खाता खोल्न लगाई उक्त खाताको डिजिटल भुक्तानी प्रणाली वा डेबिट कार्ड आफ्नो नियन्त्रणमा लिई वा विभिन्न बहानामा रकमान्तर गर्न लगाई, अवैध कारोबार गर्ने/गराउने उद्देश्यले खोलिएका मनी म्युल खाताले वित्तीय क्षेत्रको संवेदनशीलता थप बढाएको छ। संगठीत गिरोहहरूले नक्कली Know Your Customer (KYC), सीम कार्डको दुरूपयोग, बल्क मेसेजको दुरूपयोग, फेक लगानी एप जस्तै: (Smart Money Choice - SMC Scam, Telegram Based Investment Scam), अभौतिक मुद्रा (Virtual Assets) को माध्यमबाट संगठित रूपमा अत्याधुनिक प्रविधिको प्रयोग गरी अन्तरदेशीय अपराध मार्फत ठूलो रकम अवैध रूपमा बाहिरिने गरेको छ। नेपालको वित्तीय क्षेत्रमा यस किसिमका आपराधिक गतिविधिले केवल वित्तीय अपराध मात्र नभई राष्ट्रिय वित्तीय सुरक्षा, सामाजिक स्थिरता र अन्तराष्ट्रिय छविमा समेत नकारात्मक प्रभाव पार्न सक्ने देखिन्छ।

साइबर स्क्यामको असर केवल रकम गुम्नुमा मात्र सीमित नभई मध्यम र न्यून आय भएका परिवारहरूको जीवनभरको बचत एकैचोटि गुम्दा मानसिक तनाव, पारिवारिक विघटन र सामाजिक सद्भावमा समेत गम्भीर नकारात्मक असर पर्ने गरेको छ। अर्कोतर्फ, स्क्यामबाट संकलित रकम सम्पत्ति शुद्धीकरण हुँदै लागुपदार्थ कारोबार, क्रिप्टो कारोबार र अवैध रेमिट्यान्स सेटलमेन्टमा प्रयोग भइरहेको देखिन्छ। मनी म्युलका रूपमा प्रयोग गरिएका युवाहरू जान/अन्जानमा संगठित अपराधको सञ्जालमा फस्ने जोखिम बढ्दो छ।

यसै परिप्रेक्ष्यमा साइबर स्क्यामको अनुसन्धान, रोकथाम र सचेतनाको लागि बहु-निकायगत सहभागितामा आधारित, प्रविधिमैत्री र तत्काल प्रतिकार्य गर्न सक्ने चौबीसै घण्टा सञ्चालन हुने संयन्त्र एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र (IACSC) को स्थापना गर्नु अपरिहार्य रहेको छ।

२. दृष्टिकोण (Vision):

साइबर स्क्याम, ठगीजन्य कसुरको जोखिम न्यूनीकरण र प्रभावकारी अनुसन्धान गर्दै डिजिटल वित्तीय प्रणालीलाई सुरक्षित र विश्वसनीय बनाउने।

३. ध्येय (Mission):

नियामक निकाय नेपाल राष्ट्र बैंक, नेपाल दुरसञ्चार प्राधिकरण, बैंक तथा वित्तीय संस्था, भुक्तानी सेवा प्रदायक, भुक्तानी प्रणाली सञ्चालक, दूरसञ्चार सेवा प्रदायक र कानून कार्यान्वयन निकायलाई एकीकृत संयन्त्रको विकास गरी प्रचलित कानूनको परिधिभित्र रही प्रभावकारी प्रतिकार्य, स्क्यामको पूर्व संकेत/सूचना प्रवाह तथा सचेतना, रकम प्रवाह पहिचान एवम् खाता/रकम रोक्का तथा पीडितलाई रकम फिर्ता गर्न सहजीकरण गर्ने।

४. उद्देश्यहरू (Objectives):

केन्द्र स्थापनाका देहाय बमोजिमका उद्देश्यहरू रहेका छन्:

क. सामुहिक उत्तरदायित्व र जवाफदेहीतामा वृद्धि गराई साइबर स्क्याम रोकथाम र अनुसन्धानमा प्रभावकारिता ल्याउने,

ख. हटलाइन तथा अनलाइन पोर्टलसहितको उजुरी दर्ता, परामर्श र प्रारम्भिक कारबाहीका लागि चौबीसै घण्टा सञ्चालित एकल सम्पर्क बिन्दु स्थापना गर्ने,

ग. सूचना/उजुरी प्राप्त हुनासाथ स्क्याम, ठगी भएको रकम प्रवाहको बैंक खाता तथा वालेट पहिचान गरी सम्बन्धित खाता तथा रकम रोक्का गराउने प्रभावकारी प्रणाली विकास गर्ने,

घ. स्क्याममा प्रयोग भएका मोबाइल नम्बर, SIM, bulk SMS, sender-ID, phishing domain, IP, link तथा malicious application लाई नियामक एवम् सेवा प्रदायकमार्फत तत्काल निष्क्रिय गराउने,

ङ. ग्राहक पहिचान विवरण (Know Your Customer), खाता खोल्दा बखतको विवरण (Account Opening Form), बैंक स्टेटमेन्ट, तथ्याङ्क, अपराधको प्रकृति/प्रवृत्ति विश्लेषणमार्फत स्क्याम/ठगीमा प्रयोग भएका वा हुनसक्ने बैंक खाता र वालेट खाता पहिचान गरी रोक्का गर्ने,

च. प्रचलित कानूनी प्रक्रियामार्फत पीडितलाई रकम फिर्ता गराउन सहजीकरण, आवश्यक परामर्श उपलब्ध गराउने र पुनःपीडन (re-victimization) हुने जोखिमलाई न्यूनीकरण गर्ने,

छ. साइबर स्क्यामको रोकथाम तथा अनुसन्धानका लागि दिगो कानुनी र संस्थागत अधिकार सहितको प्रतिकार्य संरचना स्थापना गर्ने,

ज. राष्ट्रिय स्तरको विश्वसनीय एकद्वार प्रणाली (Single Trusted National Channel) मार्फत नागरिकमा जनचेतना अभिवृद्धि गरी साइबर स्क्याम/ठगी रोकथाम गर्ने,

झ. मनी म्युल सञ्जाल तथा स्क्यामजन्य रकम प्रवाहसम्बन्धी सूचना वित्तीय जानकारी इकाई एवम् सम्बन्धित निकायसँग आदानप्रदान गरी राष्ट्रिय AML/CFT प्रणालीलाई सुदृढ बनाउन योगदान पुऱ्याउने,

ञ. अन्तराष्ट्रिय संस्था र अन्य देशहरूसंग समन्वय गरी साइबर स्क्याम/ठगी कसुरको अनुसन्धानलाई प्रभावकारी बनाउन।

५. कार्यक्षेत्र (Scope):

यस केन्द्र (IACSC) को कार्यक्षेत्र निम्नानुसार रहनेछ।

क. हटलाइन तथा अनलाइन पोर्टलमार्फत डिजिटल स्क्यामसम्बन्धी उजुरीको दर्ता, वर्गीकरण र प्राथमिकीकरण,

ख. स्क्याम भएको वा ठगिएको रकम प्रवाह तथा अन्तिम लाभ् लिने खाता/वालेटको पहिचान,

ग. सम्बन्धित बैंक, वित्तीय संस्थामार्फत खाता तथा रकम रोक्का (debit freeze/lien marking) को समन्वय र अभिलेखीकरण,

घ. स्क्याममा प्रयोग भएका मोबाइल नम्बर, SIM, sender-ID, domain, IP हरूको निष्क्रियता,

नेपाल प्रहरी
गृह मन्त्रालय

शेरबहादुर थापा
सचिव

ङ. मनी म्युल खाता तथा वालेटको सञ्जाल विश्लेषण तथा जोखिम सूची (watch list) व्यवस्थापन,

च. Smishing, Vishing, Phishing लगायतका साइबर स्क्याम र ठगी पहिचान गर्ने प्रणालीको विकास,

छ. स्क्याम/ठगीको प्रक्रिया चलिरहेकै अवस्थामा सम्भावित पीडितलाई SMS वा कलमार्फत तत्काल सचेत गराई कारोबार रोक्न सहजीकरण,

ज. साइबर स्क्याम, फ्रडका नयाँ स्वरूप (typology) को अध्ययन, प्रवृत्ति विश्लेषण र वार्षिक प्रतिवेदन,

झ. सम्बन्धित प्रहरी कार्यालय एवम् अभियोजन निकायलाई प्राविधिक सहयोग तथा प्रमाण हस्तान्तरण,

ञ. पीडितलाई प्रक्रियागत परामर्श, उजूरी उपर कारबाहीको जानकारी (case tracking) र रकम फिर्ता सम्बन्धी सहजीकरण,

ट. रकम स्थानान्तरण गरी अभौतिक मुद्रामा (Virtual Assets) रुपान्तरण गर्न सक्ने संभावनाको पहिचान तथा सम्बन्धित निकायसँग समन्वय र रोकथाम,

ठ. नियामक निकायलाई प्रणालीगत जोखिम सम्बन्धी सूचना र नीतिगत सुधारको लागि सिफारिस,

ड. साइबर स्क्याममा प्रयोग भएका सामाजिक सञ्जालका एकाउन्ट, ह्याण्डल, आइडी, ग्रुप, प्रोफाईल आदीको पहिचान, प्रमाण संकलन र निष्क्रिय (Takedown) गर्न आवश्यक समन्वय,

ढ. सार्वजनिक सचेतना, पूर्व सतर्कता सूचना प्रवाह,

ण. साइबर फ्रड/स्क्यामको रकम देश बाहिर पुगेको अवस्थामा वा देश बाहिरबाट आपराधिक गतिविधि भएको अवस्थामा पारस्परिक कानुनी सहायता (Mutual Legal Assistance) मार्फत समन्वय गर्ने, INTERPOL तथा अन्य मुलुकका समकक्षी संयन्त्रसँग कानूनको अधिनमा रही सूचनाको आदानप्रदान।

६. कार्यगत संरचना (Working Structure)

यस केन्द्रको दैनिक कार्य सञ्चालन, जनशक्ति परिचालन, व्यवस्थापन, निर्देशन, अनुगमन, सुपरीवेक्षण समेतको लागि निम्नानुसारको तीन तहको संरचना रहनेछ।

क. निर्देशक समिति (Steering Committee):

(१) बहुनिकाय संलग्न भई कार्य सम्पादन गर्नुपर्ने यो प्रणालीमा मौजुदा कानून एवम् कार्ययोजना कार्यन्वयनमा सहजीकरण गरी नियमित रुपमा समीक्षा, मुल्याङ्कन, नीतिगत निर्देशन र अन्तर-मन्त्रालय समन्वय लगायतका कार्य गर्न गृह मन्त्रालयको सह-सचिवको संयोजकत्वमा देहाय बमोजिमको निर्देशक समिति रहनेछ।

सह-सचिव, सुरक्षा तथा समन्वय महाशाखा, गृह मन्त्रालय	-	संयोजक
सह-सचिव, अर्थ मन्त्रालय	-	सदस्य
सह-सचिव, कानून महाशाखा, गृह मन्त्रालय	-	सदस्य

नेपाल सरकार
गृह मन्त्रालय

उदारनाथ रा
सचिव

सह-सचिव, सूचना प्रविधि तथा विद्युतीय शासन कार्यालय	-	सदस्य
महानिर्देशक सम्पत्ति शुद्धीकरण अनुसन्धान विभाग	-	सदस्य
सह-न्यायधिवक्ता, महान्याधिवक्ता कार्यालय	-	सदस्य
निर्देशक, भुक्तानी प्रणाली विभाग, नेपाल राष्ट्र बैंक,	-	सदस्य
प्रमुख, वित्तीय जानकारी इकाई, नेपाल राष्ट्र बैंक	-	सदस्य
प्रमुख, साइबर ब्यूरो, नेपाल प्रहरी प्रधान कार्यालय	-	सदस्य
निर्देशक, नेपाल दुरसंचार प्राधिकरण	-	सदस्य
अध्यक्ष, नेपाल बैंकर्स संघ	-	सदस्य
अध्यक्ष, इन्टरनेट सेवा प्रदायक संघ	-	सदस्य

उप-सचिव, शान्ति सुरक्षा तथा अपराध नियन्त्रण शाखा, गृह मन्त्रालय - सदस्य सचिव

(२) यस निर्देशक समितिको सचिवालय गृह मन्त्रालयमा रहनेछ।

(३) समितिको कार्यसम्पादनका क्रममा विभिन्न सरोकारवाला मन्त्रालय, निकाय, संस्था तथा अन्य सम्बन्धित पक्षबीच आवश्यक समन्वय, सहकार्य तथा संयोजन गर्ने कार्य गृह मन्त्रालयले गर्नेछ । समितिका पदाधिकारीहरूले प्रचलित कानूनबमोजिम आफू कार्यरत संस्था वा निकायलाई प्राप्त अधिकारको प्रयोग तथा आफ्नो जिम्मेवारीको निर्वाह गर्दा सम्बन्धित संस्था वा निकायप्रति उत्तरदायी रहनेछन्।

(४) निर्देशक समितिको बैठक छ (६) महिनामा कम्तिमा एक पटक र विषयको गाम्भिर्यता अनुरूप आवश्यकता देखिएमा जुनसुकै बेला बैठक बस्न सक्नेछ।

(५) यस समितिको काम कर्तव्य र अधिकार देहाय बमोजिम हुनेछ ।

क. साइवर स्क्याम, ठगीको रोकथाम तथा अनुसन्धान सम्बन्धी रणनीतिक प्राथमिकता निर्धारण गर्ने,

ख. साइबर स्क्याम प्रतिकार्य केन्द्रको स्थापना, सञ्चालन, विस्तार र संस्थागत सुदृढीकरणसम्बन्धी नीतिगत मार्गदर्शन प्रदान गर्न,

ग. साइबर स्क्याम, ठगी सम्बन्धी रकम रोक्का, रकम फिर्ता (बैंक, वालेट, दुरसञ्चार सेवा टपअप समेत) र पीडित संरक्षणसम्बन्धी समन्वय र सहजिकरण गर्ने,

घ. केन्द्रका लागि आवश्यक कानुनी, नीतिगत तथा संरचनागत सुधारको पहिचान गरी आवश्यकता अनुसार गृह मन्त्रालयमा सिफारिस गर्ने,

ङ. सहभागी निकायहरूबीच प्रभावकारी समन्वय, सहकार्य र सूचना आदान-प्रदानको व्यवस्था सुनिश्चित गर्ने,

च. केन्द्रको वार्षिक नीति, कार्ययोजना, प्राथमिकता र कार्यसम्पादन सूचकहरू स्वीकृत गर्ने,

नेपाल सरकार
गृह मन्त्रालय

सचिव

छ. कार्यसम्पादन प्रतिवेदन, प्रगति विवरण तथा उपलब्धि समीक्षा गरी आवश्यक सुधारात्मक निर्देशन दिने,

ज. केन्द्रको लागि आवश्यक स्रोत साधन, जनशक्ति, प्रविधि, पूर्वाधार र बजेट व्यवस्थापन सम्बन्धी निर्णय गर्ने,

झ. साइबर स्क्यामको प्रवृत्ति, जोखिम, चुनौती र राष्ट्रिय/अन्तर्राष्ट्रिय अभ्यासको समीक्षा गरी उपयुक्त नीति तय गर्ने,

ञ. नेपाल सरकार तथा सम्बद्ध निकायबाट प्राप्त हुन आएका निर्देशन लगायत अन्य कार्यक्रमहरू कार्यान्वयन तथा सञ्चालन गर्ने,

ट. कार्यान्वयन तहको समन्वय र सहकार्यलाई प्रभवकारी बनाउन आवश्यक अन्य कार्य गर्ने गराउने।

(६) निर्देशक समितिले सम्बद्ध निकायको पदाधिकारी वा विज्ञलाई आवश्यकता अनुसार बैठकमा आमन्त्रण गर्न सक्नेछ।

ख. सञ्चालन समन्वय समिति (Operations Coordination Committee):

(१) एकिकृत साइबर स्क्याम प्रतिकार्य केन्द्र (IACSC) को कार्य प्रभावकारिता अभिवृद्धि गर्नको लागि कार्यगत समन्वय कायम गर्न वा गराउन देहाय बमोजिमको सञ्चालन समन्वय समिति रहने छ।

क. निर्देशक, भुक्तानी प्रणाली विभाग, नेपाल राष्ट्र बैंक	-	संयोजक
ख. निर्देशक, राष्ट्रिय साइबर सुरक्षा केन्द्र	-	सदस्य
ग. निर्देशक, सम्पत्ति शुद्धीकराण अनुसन्धान विभाग	-	सदस्य
घ. निर्देशक, राष्ट्रिय सहकारी नियमन प्राधिकरण	-	सदस्य
ङ. उपन्यायाधिवक्ता, महान्याययाधिवक्ताको कार्यालय	-	सदस्य
च. प्रहरी उपरीक्षक, एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र	-	सदस्य
छ. उप-निर्देशक, नेपाल दुरसञ्चार प्राधिकरण	-	सदस्य
ज. अध्यक्ष, नेपाल मुद्रा विप्रेषक संघ	-	सदस्य
झ. अध्यक्ष, डेभलपमेन्ट बैंकर्स एशोसियसन नेपाल	-	सदस्य
ञ. अध्यक्ष, नेपाल वित्तीय संस्था संघ	-	सदस्य
ट. प्रतिनिधि, नेपाल बैंकर्स सघं	-	सदस्य
ठ. प्रतिनिधि, भुक्तानी सेवा प्रदायक संघ	-	सदस्य
ड. प्रतिनिधि, भुक्तानी प्रणाली संचालक	-	सदस्य
ढ. प्रतिनिधि, इन्टरनेट सेवा प्रदायक संघ	-	सदस्य
ण. उप-निर्देशक, भुक्तानी प्रणाली विभाग, नेपाल राष्ट्र बैंक	-	सदस्य सचिव

नेपाल सरकार
गृह मन्त्रालय

देवराज [illegible]
[illegible]

(२) यस सञ्चालन समन्वय समितिको सचिवालय नेपाल राष्ट्र बैंकमा रहनेछ।

(३) सञ्चालन समन्वय समितिको बैठक तीन (३) महिनामा कम्तिमा एक पटक र विषयको गाम्भिर्यता अनुरूप आवश्यकता देखिएमा जुनसुकै बेला बैठक बस्न सक्नेछ।

(४) यस समितिको काम कर्तव्य र अधिकार देहाय बमोजिम हुनेछ।

क. केन्द्रको सञ्चालनलाई प्रभावकारी, छरितो र समन्वयात्मक बनाउने,

ख. सरोकारवाला निकायहरुबीच निरन्तर कार्यगत समन्वय कायम गर्ने,

ग. साइबर स्क्यामसम्बन्धी उजुरी, रकम रोक्का, खाता फुकुवा, मनी ट्रेल विश्लेषण तथा प्रमाण संकलनसम्बन्धी कार्यमा आवश्यक सहजीकरण गर्ने,

घ. केन्द्रमा कार्यरत Co-Located Officers र प्रणालीमा जोडिएका अधिकार प्राप्त समन्वय अधिकारीहरूको समन्वयात्मक रूपमा कार्यसम्पादन र समन्वयको अनुगमन गर्ने,

ङ. केन्द्रबाट सञ्चालन हुने कार्य सञ्चालन प्रवाह, कार्यविधि, प्रतिवेदन फर्मेट, उजुरीको जानकारी गराउने प्रणाली तथा काम कारवाहीको प्रभावकारीता सुनिश्चित गर्ने,

च. रकम रोक्का, जोखिमयुक्त खाता पहिचान, नम्बर/SIM निष्क्रियता, Domain/IP Block, तथा अन्य तात्कालिक प्रतिकार्य कार्यमा आवश्यक समन्वय गर्ने,

छ. केन्द्रको कार्यसम्पादनमा देखिएका प्राविधिक, प्रशासनिक, कार्यगत समस्या पहिचान गरी निर्देशन समिति समक्ष प्रस्ताव गर्ने,

ज. एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रको कार्यसम्पादन, अधिकारको प्रयोग, उजुरी सुन्ने Oversight Mechanism को रूपमा कार्य गर्ने,

झ. आवश्यक स्रोत, साधन, प्रविधि, बजेट, योजना सम्बन्धी प्रस्ताव निर्देशक समितिमा पेस गर्ने,

ञ. प्रगति समीक्षा र सोको प्रतिवेदन आवश्यकता अनुसार निर्देशक समितिमा पेस गर्ने,

ट. उजुरीको प्रकृति, प्रवृत्ति र जोखिम विश्लेषणका आधारमा सुधारात्मक उपायहरू सुझाव दिने,

ठ. सार्वजनिक सचेतना, प्रारम्भिक चेतावनी र जोखिम न्यूनीकरणका लागि सामग्रीहरू प्रचार-प्रसार गर्ने,

ड. केन्द्रमा काम गर्ने कर्मचारीहरूले पालना गर्नुपर्ने आचारसंहिता (Code of Conduct) तयार गरी स्विकृतिको लागी निर्देशक समिति समक्ष पेस गर्ने,

ढ. केन्द्रमा रहने कर्मचारीहरूको क्षमता अभिवृद्धिको लागि योजना निर्माण तथा कार्यक्रम सञ्चालन गर्ने,

ण. स्क्याम/फ्रडको प्रकृति, प्रवृत्ति र चाप अनुसार एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रमा रहने कर्मचारीहरूको संख्या लगायत अन्य आवश्यक संशोधन (Amendment) गर्नुपर्ने आवश्यकता भएमा औचित्य खुलाई निर्देशक समिति समक्ष स्विकृतीका लागि पेस गर्ने,

त. सञ्चालन समन्वय समिति आफ्नो काम कारवाहीको सन्दर्भमा निर्देशक समिति प्रति उत्तरदायी रहनेछ।

(५) समन्वय समितिले सम्बद्ध निकायको पदाधिकारी वा विज्ञलाई आवश्यकता अनुसार बैठकमा आमन्त्रण गर्न सक्नेछ।

ग. एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र (Integrated Anti Cyber Scam Center):

(१)दैनिक कार्य सञ्चालनका लागि खटिएका र प्रणालीमा जोडिएका अधिकार प्राप्त समन्वय अधिकारीहरू (Co-located Officers) २४ सै घण्टा समन्वयात्मक रूपमा कार्यसम्पादन गर्नको लागि नेपाल प्रहरी प्रधान कार्यालय, साइबर ब्यूरोमा एक एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र रहने छ।

(२)केन्द्रको दैनिक कार्य सञ्चालनार्थ नेपाल प्रहरीका प्रहरी उपरीक्षक केन्द्रको संयोजक रहने छन्।

(३)यस केन्द्रको कार्यसम्पादनलाई प्रविधिमैत्री एवम् प्रभावकारी बनाउन हाल निर्माणाधीन सफ्टवेयर (OFFERS) निर्माण पश्चात यसै केन्द्रबाट सञ्चालन हुनेछ।

(४)यस केन्द्रको काम कर्तव्य र अधिकार देहाय बमोजिम हुनेछ।

क. केन्द्रमा प्राप्त साइबर स्क्याम, ठगीसम्बन्धी उजुरी दर्ता, वर्गीकरण, प्राथमिकीकरण गर्ने,

ख. उजुरी प्राप्त हुनासाथ सम्बन्धित खाता, वालेट, रकम प्रवाहको तत्काल पहिचान तथा विश्लेषण गर्ने,

ग. सम्बन्धित बैंक, वित्तीय संस्था, भुक्तानी सेवा प्रदायक, भुक्तानी प्रणाली सञ्चालक, दूरसञ्चार सेवा प्रदायकसँग तत्काल समन्वय गरी कानून वमोजिम खाता रोक्का, फुकुवा, नम्बर/SIM निष्क्रियता, domain/IP block तथा log preservation गराउने,

घ. स्क्याममा प्रयोग भएका beneficiary account, mule account, wallet, device, SIM, sender ID, phishing link, malicious app, social media account लगायतका माध्यमको पहिचान, अभिलेखीकरण र विश्लेषण गर्ने,

ङ. सम्भावित पीडितलाई तत्काल SMS, कल वा अन्य माध्यमबाट सतर्क गराई थप रकम स्थानान्तरण रोक्न सहजीकरण गर्ने,

च. साइबर स्क्याम/फ्रड कसुरसँग सम्बन्धित रकमको रोक्का, फुकुवा, प्रमाण संकलन र अनुसन्धानका लागि आवश्यक कागजात तयार गर्ने,

केदारनाथ [illegible]
सचिव

छ. सम्बन्धित प्रहरी अनुसन्धान इकाइलाई प्रमाण, तथ्याङ्क र प्राविधिक विवरण हस्तान्तरण गर्ने,

ज. पीडितलाई उजुरीको अवस्था, रोक्का/फुकुवाको अवस्था र अनुसन्धान प्रगति सम्बन्धी जानकारी उपलब्ध गराउने,

झ. मनी म्युल सञ्जाल, नयाँ typology, प्रवृत्ति, जोखिम र उदीयमान स्क्याम ढाँचाको अध्ययन तथा विश्लेषण गर्ने,

ञ. सार्वजनिक सचेतना, प्रारम्भिक चेतावनी र जोखिम न्यूनीकरणका लागि सामग्री तयार पारी सञ्चालन समन्वय समितिमा सिफारिस गर्ने,

ट. IACSC तथा ISP बीच API, डेटा आदान—प्रदान, IP/डोमेन ब्लकिङ, लग संरक्षण र सूचना व्यवस्थापन लगायतका मापदण्डको मस्यौदा तयार गरी सञ्चालन समन्वय समितिमा पेस गर्ने,

ठ. केन्द्र सञ्चालनको लागि आवश्यक पर्ने जनशक्ति, प्रविधि, तालिम, बजेट कार्यक्रमबारे सञ्चालन समन्वय समितिमा जानकारी गराउने,

ड. दैनिक सञ्चालनसम्बन्धी तथ्याङ्क, कार्यसम्पादन र प्रतिकार्यको अभिलेख राख्ने,

ढ. समन्वय अधिकारीहरूबीच कार्यविभाजन, उपस्थिति र कार्यप्रवाह सुनिश्चित गर्ने,

(५)दैनिक काम कारवाहीको सन्दर्भमा सञ्चालन समन्वय समिति प्रति उत्तरदायी रहनेछ।

(६)केन्द्रको दैनिक कार्यसञ्चालको क्रममा विषय विज्ञ एवम् प्रशिक्षार्थी विद्यार्थी (Intern Student) हरूलाई समन्वय समितिबाट अनुमति प्राप्त गरी केन्द्रको कार्यमा संलग्न गर्न सकिनेछ ।

७. एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रमा रहने निकायहरूको भूमिका र जिम्मेवारी (Role and Responsibilities):

एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र (IACSC) मा नियामक निकाय, बैङ्क तथा वित्तीय संस्था, सेवा प्रदायक संस्था, भुक्तानी प्रणाली सञ्चालक र कानून कार्यान्वयन गर्ने निकायहरू एउटै भौतिक कक्षमा रहनेछन्। केन्द्रमा रहने अधिकारप्राप्त अधिकारीहरू (Co-located officers) हरूको भूमिका र जिम्मेवारी देहाय बमोजिमका रहनेछ।

सहभागी निकाय	IACSC मा भूमिका र जिम्मेवारी
नेपाल प्रहरी	केन्द्रको संयोजन, उजुरी दर्ता, समन्वय तथा प्राथमिकीकरण, अनुसन्धान, कार्य सञ्चालन समन्वय संयन्त्रको व्यवस्थापन एवम् प्रमाण संरक्षण ।
नेपाल राष्ट्र बैंक	नियामकीय निर्देशन तथा मापदण्ड निर्धारण, खाता तथा रकम रोक्काको आधार, अवधि एवम् प्रक्रिया निर्धारण, बैंक तथा भुक्तानी सेवाप्रदायकको अनुगमन ।
बैंक तथा वित्तीय संस्था (क वर्ग)	Co-located अधिकृतको व्यवस्था, म्युल खाताको पहिचान, खाता तथा रकम रोक्का, फुकुवा, KYC/AOF, बैंक स्टेटमेन्ट, IP Log को विश्लेषण गर्ने र उच्च जोखिमयुक्त कारोबारको निगरानी ।

नेपाल सरकार
गृह मन्त्रालय

केदारनाथ शर्मा
सचिव

सहभागी निकाय	IACSC मा भूमिका र जिम्मेवारी
भुक्तानी सेवा प्रदायक (PSPs)	वालेट खाता वा रकम रोक्का, फुकुवा, म्युल खाताको पहिचान, KYC/AOF, कारोबार विवरण, IP Log को विश्लेषण गर्ने र उच्च जोखिमयुक्त कारोबारको निगरानी ।
भुक्तानी सेवा सञ्चालक (PSOs)	रकम प्रवाहको निगरानी, IP Log र कारोबार विवरण उपलब्ध, उच्च जोखिमयुक्त कारोबारको निगरानी
डेभलपमेन्ट बैंकर्स एशोसियसन नेपाल	समन्वय/सम्पर्क अधिकृतको व्यवस्था, म्युल खाताको पहिचान, खाता तथा रकम रोक्का, फुकुवा, KYC/AOF, बैंक स्टेटमेन्ट, IP Log को विश्लेषण गर्ने र उच्च जोखिमयुक्त कारोबारको निगरानी ।
दूरसञ्चार सेवा प्रदायक संस्थाहरु	स्क्याममा प्रयोग भएको मोबाइल नम्बर तथा सिमकार्ड पहिचान गर्ने, निष्क्रिय गराउने, Calling Line Identification (CLI) spoofing, bulk SMS र sender-ID को दुरुपयोग नियन्त्रण लगायतका साइबर स्क्याम नियन्त्रणको लागि आवश्यक समन्वय । Phishing तथा fraudulent domain र IP को अवरोध, log preservation, malicious application र सर्भरसम्बन्धी प्राविधिक सूचना आदानप्रदान ।

८. एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रको जनशक्ति व्यवस्थापन:

क. प्रहरी उपरीक्षकको संयोजकत्वमा केन्द्र चौबीसै घण्टा (२४X७) सञ्चालन हुनेछ।

ख. उजुरी दर्ता, वित्तीय अनुसन्धान, साइबर विश्लेषण एवम् केन्द्रको अन्य कार्य सञ्चालनका लागि केन्द्रले तीन (३) सिफ्टमा कार्य सम्पादन गर्नेछ।

ग. केन्द्रमा नै Co-Located अधिकारीको रूपमा नेपाल राष्ट्र बैंक, नेपाल प्रहरी, "क" वर्गका वाणिज्य बैंक, दुरसञ्चार सेवा प्रदायक संस्था, डेभलपमेन्ट बैंकर्स एशोसियसन नेपाल र भुक्तानी सेवा प्रदायकका खल्ती र ई-सेवा समेतका पदाधिकारीहरु रहनेछन्।

घ. बैंक तथा वित्तीय संस्था, भुक्तानी सेवा प्रदायक संस्था र भुक्तानी प्रणाली सञ्चालकबाट प्रतिनिधिको रूपमा खटिने Co-Located अधिकारीको समन्वय नेपाल राष्ट्र बैंकले गर्नेछ।

ङ. दुरसञ्चार सेवा प्रदायक संस्थाबाट प्रतिनिधिको रूपमा खटिने Co-Located अधिकारीको समन्वय नेपाल दुरसञ्चार प्राधिकरणले गर्नेछ।

च. एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रमा नै Co-located अधिकारीको रूपमा रहने निकाय बाहेकका अन्य बैंक तथा वित्तीय संस्थाहरू २४ सै घण्टा आ-आफ्नै कार्यालयबाट यस केन्द्रको समन्वयमा कार्यसम्पादन गर्नेछन्। यसरी आ-आफ्नो कार्यालयबाट कार्य-सम्पादन गर्ने अधिकारीहरूको फोन नं र इमेल ठेगाना स्थायी हुने र सोही मार्फत २४ सै घण्टा सम्पर्क र समन्वय हुने सुनिश्चितता गरिनेछ। घटनाको प्रकृति र अवस्था अनुसार कुनै पनि बैंक वित्तीय संस्थाका समन्वय अधिकृतहरु आवश्यकता अनुसार केन्द्रमा नै उपस्थित भई Co-located अधिकारीको रुपमा कार्य सम्पादन गर्नुपर्नेछ।

छ. तर, यस एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रमा उपस्थिति भई कार्य गरिरहेको अवस्थामा OFFERS सफ्टवेयर पूर्ण कार्यान्वयनमा आएपश्चात कुनै सरोकारवाला निकाय/संस्थाले प्रविधि

नेपाल सरकार
गृह मन्त्रालय

केदारमणि पाण्डे
सचिव

मार्फत यस केन्द्रको लक्ष्य हासिल गर्न २४ सै घण्टा (२४/७) भौतिक रूपमा उपस्थित भए सरहको कार्य सम्पादन गर्ने सुनिश्चिता गरेमा केन्द्रमा भौतिक रूपमा उपस्थिति अनिवार्य नहुन सक्दछ।

ज. एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रमा रहने कर्मचारीहरूको संख्यागत विवरण निम्नानुसार हुनेछ।

सि.नं.	संस्था/निकाय	एक सिफ्ट	दैनिक कूल जनशक्ती	कैफियत
१.	नेपाल प्रहरी	९ जना	३३ जना (दैनिक कार्य सञ्चालनका लागि आवश्यक ६ जना कर्मचारी समेत)	नेपाल प्रहरीबाट केन्द्रका लागि आवश्यक जनशक्तिको तत्कालको लागि नेपाल प्रहरीको विद्यमान जनशक्तिबाट व्यवस्थापन गर्ने।
२.	नेपाल राष्ट्र बैंक	१ जना	३ जना	आवश्यकता अनुसार भौतिक रुपमा प्रतिकार्य केन्द्रमा उपस्थित हुने
३.	"क" वर्गका बैंक	२० जना	६० जना	
४.	नेपाल टेलिकम, एनसेल	१/१ जना गरी २ जना	६ जना	
५.	इन्टरनेट सेवा प्रदायक संघ	१ जना	३ जना	सबै इन्टरनेट सेवा प्रदायक संघमा आवद्ध भएका तथा नभएका सेवा प्रदायकबाट 24/7 Dedicated Focal Person तोकिने।
६.	डेभलपमेन्ट बैंकर्स एशोसियसन नेपाल	१ जना	३ जना	सबै डेभलपमेन्ट बैंकबाट 24/7 Dedicated Focal Person तोकिने।
७.	भुक्तानी सेवा प्रदायक खल्ती र ई-सेवा	१/१ जना गरी २ जना	६ जना	अन्य भुक्तानी सेवा प्रदायकबाट 24/7 Dedicated Focal Person तोकिने
जम्मा		३६ जना	११४ जना	

झ. एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रमा रहने कर्मचारीहरूको संख्या स्क्याम/ठगीको प्रकृत्ति, प्रवृत्ति र चाप अनुसार सञ्चालन समन्वय समितिको सिफारिसमा निर्देशक समितिले फेरबदल गर्न सक्नेछ।

९. कार्य सञ्चालन प्रवाह (Workflow):

एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्रले साइबर स्क्याम रोकथाम र अनुसन्धान कार्य प्रभावकारी बनाउनको लागि देहाय बमोजिम कार्य सञ्चालन गर्नेछ।

क. उजुरी दर्ता र प्राथमिकीकरण (०-१० मिनेट) :

केदारलाल राजी
सचिव

हटलाइन (Emergency/आकस्मिक प्रयोजनको लागि), सूचना प्रवाह लाईन (Non-Emergency/सूचना आदान प्रदान र उजुरी फ्लोअपको लागि), नागरिक एप, Nepal Police App, प्रतिकार्य केन्द्रको अनलाइन पोर्टल, वा अन्य माध्यममार्फत प्राप्त उजुरी यस केन्द्रको उजूरी/मुद्दा व्यवस्थापन प्रणालीमा दर्ता भई Reference number सिर्जना हुनेछ र फ्रड/स्क्यामको प्रकृति र प्रवृत्ति हेरी घटनाको प्राथमिकीकरण (triage) गर्ने।

ख. पहिचान (१०-३० मिनेट) :

बैंक, भुक्तानी सेवा प्रदायक संस्था र भुक्तानी प्रणाली संचालक संस्थाका समन्वय अधिकृतले लाभग्राही खाता, वालेट खाताको कारोबार समय र रकम प्रवाहको ट्रेल तत्काल पहिचान गर्ने।

ग. (१०-६० मिनेट):

प्रचलित कानुन बमोजिम सम्बन्धित बैंक वा वालेट खाता तथा रकम रोक्का अनुरोध एकैपटक प्रवाह गर्ने तथा अन्य खातामा रकमान्तर भइसकेको अवस्थामा मनी ट्रेल पछ्याई क्रमिक रूपमा खाता वा रकम रोक्का गर्ने।

घ. स्क्याममा प्रयोग भएको सञ्चार माध्यम अवरोध (१०-६० मिनेट):

स्क्याम भएको रकमको ट्रेल अनुसन्धान गर्दै गर्दा समानान्तर रूपमा प्रचलित कानून बमोजिम मोबाईल सेवा प्रदायक मार्फत सिम निष्क्रिय गर्ने र इन्टरनेट सेवा प्रदायक मार्फत phishing domain र IP block एवम् log preservation सुनिश्चित गर्ने।

ङ. अनुसन्धान:

यस केन्द्रले उपलब्ध गराएको कागजात तथा प्रमाणको आधारमा सम्बन्धित प्रहरी अनुसन्धान कार्यालयबाट रकम फिर्ता एवम् आवश्यकता अनुसार थप अनुसन्धान हुनेछ।

च. पीडितसँग सञ्चार:

उजुरी दर्ता, रोक्का अनुरोध, रोक्काको नतिजा र अनुसन्धान प्रारम्भ गरी प्रत्येक चरण परिवर्तनमा पीडितलाई सूचित गर्ने र उजुरी/निवेदनबारे सूचना आदान प्रदान गर्ने सुविधा उपलब्ध गराउने।

छ. फिर्ता र फकुवा :

प्रचलित कानूनबमोजिम अदालतको आदेशमार्फत पीडितलाई रकम फिर्ता गराउने र निर्दोष तेस्रो पक्षको खाता अनावश्यक रूपमा रोकिएको भए तत्काल फुकुवा गर्ने।

ज. पृष्ठपोषण (Feedback Loop) :

प्रत्येक घटनाबाट प्राप्त Typology लाई प्रवृत्ति विश्लेषण, सार्वजनिक सचेतना र नियामकीय सुधारमा रूपान्तरण गर्ने।

नेपाल सरकार
गृह मन्त्रालय

केदारनाथ शर्मा
सचिव

IACSC को कार्य सञ्चालन प्रवाह

उजुरी प्राप्ति
हटलाइन, अनलाइन पोर्टल, मोबाइल एप, नजिकको प्रहरी इकाई

▼

दर्ता तथा प्राथमिकीकरण (० — १० मिनेट)
Case ID सिर्जना र प्राथमिकीकरण

▼

रकम प्रवाहको पहिचान (१० — ३० मिनेट)
बैंक तथा PSP/PSOs सम्पर्क अधिकृतबाट Beneficiary खाता, Wallet ID र Money Trail

▼

रोक्का (१० — ६० मिनेट)	अवरोध (१०-६० मिनेट)
Debit Freeze, Lien Marking, Layered Account सम्म क्रमिक रोक्का	नम्बर तथा SIM निष्क्रिय, Domain र IP अवरोध, Log Preservation

▼

अनुसन्धान हस्तान्तरण
मुद्दा दर्ता, प्रमाण सङ्कलन र सम्बन्धित प्रहरी कार्यालयमा हस्तान्तरण

▼

रकम फिर्ता तथा फुकुवा
कानून वमोजिम पीडितलाई रकम फिर्ता (बैंक, वालेट, दुरसञ्चार टपअप), निर्दोष खाता तत्काल फुकुवा

▼

पृष्ठपोषण
Typology विश्लेषण, सार्वजनिक सचेतना र नियामकीय सिफारिस

▼

समानान्तर : पीडितसँग निरन्तर सञ्चार
नियमित अपडेट र Case Tracking सुविधा

१०. प्रतिवेदन प्रणाली (**Reporting System**):

क. केन्द्रको संयोजकले सञ्चालन समन्वय समिति संयोजकको प्रत्यक्ष सुपरिवेक्षणमा रही कार्यसम्पादन गर्नेछ।

नेपाल सरकार गृह मन्त्रालय

केदारनाथ शर्मा
सचिव

ख. केन्द्र संयोजकले मासिक प्रगति प्रतिवेदन सञ्चालन समन्वय समिति समक्ष पेस गर्नेछ भने सञ्चालन समन्वय समितिले त्रैमासिक समीक्षा प्रतिवेदन निर्देशक समिति (Steering Committee) समक्ष पेस गर्नेछ।

ग. निर्देशक समितिले वार्षिक प्रतिवेदन गृह मन्त्रालयमा पेस गर्नुपर्नेछ।

११. कानुनी आधार (Legal Framework):

विद्यमान कानूनी संरचनाले अनुसन्धान, नियमन तथा कारबाहीका लागि आधार प्रदान गरे अनुरूप केन्द्रले देहायका कानूनी व्यवस्थाको अधिनमा रही यस दिग्दर्शन बमोजिम कार्य सञ्चालन गर्नेछ।

क. नेपाल राष्ट्र बैंक ऐन, २०५८,

ख. भुक्तानी तथा फछ्यौंट ऐन, २०७५,

ग. बैंक तथा वित्तीय संस्था सम्बन्धी ऐन, २०७३,

घ. सम्पत्ति शुद्धीकरण निवारण ऐन, २०६४,

ङ. बैकिङ् कसूर तथा सजाय ऐन, २०६४,

च. विद्युतीय कारोबार ऐन, २०६३,

छ. सहकारी ऐन, २०७४,

ज. मुलुकी अपराध संहिता, २०७४,

झ. नेपाल राष्ट्र बैंक, बैंक तथा वित्तीय संस्था नियमन विभाग, बैंक खाता रोक्का तथा फुकुवा सम्बन्धी विनियमावली, २०८१,

ञ. नेपाल राष्ट्र बैंक, बैंक तथा वित्तीय संस्था नियमन विभाग, एकिकृत निर्देशन २०८२,

ट. सूचना पहुँच सम्बन्धी (कार्यविधि) निर्देशिका २०७४,

ठ. राष्ट्रिय साईबर सुरक्षा नीति-२०८०,

ड. अन्य प्रचलित कानूनहरू।

१२. स्रोत व्यवस्थापन (Resource Management):

एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र (IACSC) को स्थापना, पूर्वाधार विकास, आवश्यक प्रविधि तथा प्रणालीको व्यवस्थापन र सञ्चालनका लागि आवश्यक पर्ने बजेट नेपाल सरकारबाट विनियोजन हुनेछ।

१३. क्षमता विकास (Capacity Development)

केन्द्रमा रहने कर्मचारीहरूलाई आवश्यक पर्ने आधारभूत तथा विशिष्टिकृत तालिमहरू प्रदान गर्न केन्द्रले निर्देशक समितिको समन्वयमा आवश्यक व्यवस्था मिलाउनेछ। क्षमता अभिवृद्धि सम्बन्धी सम्पुर्ण प्रशासनिक, आर्थिक र व्यवस्थापकीय जिम्मेवारी निर्देशक समितिको सिफारिसमा नेपाल सरकारले गर्नेछ।

नेपाल सरकार
गृह मन्त्रालय

केशरलाल श्रेष्ठ
सचिव

१४. गोपनियता (Confidentiality):

यस केन्द्रमा रहने कर्मचारीहरूले देहाय अनुसार गोपनीयता कायम गर्नु पर्नेछ।

क. निर्देशक समितिबाट जारी हुने आचार संहिता,

ख. स्क्याम/फ्रड अनुसन्धान सम्बन्धी सुचनाको गोप्यता,

ग. Digital Evidence को सुरक्षित प्रणालीमा भण्डारण,

घ. Role wise Access Control ।

१५. सिमा (Limitation):

अनलाइन साइबर स्क्याम, अनलाईन ठगी बाहेकका अन्य कसुरमा एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र (Integrated Anti-Cyber Scam Center - IACSC) को स्थापना र सञ्चालन सम्बन्धी दिग्दर्शनका प्रावधानहरू लागू हुने छैन । प्रचलित कानुन, नेपाल राष्ट्र बैंकबाट जारी भएका निर्देशनहरूको परिधिमा रही यस केन्द्रले काम-कारवाही सञ्चालन गर्नेछ।

१६. संशोधन र खारेजी (Amendment and Repel):

सूचना प्रविधिको साथसाथै साइबर स्क्याम/ठगीको प्रकृति र प्रवृतिमा आउने परिवर्तन अनुसार आवश्यकता बमोजिम एकीकृत साइबर स्क्याम प्रतिकार्य केन्द्र (Integrated Anti-Cyber Scam Center - IACSC) को सञ्चालन सम्बन्धी व्यवस्थामा निर्देशक समितिको सिफारिसमा गृह मन्त्रालयले संशोधन र खारेजी गर्नेछ।

नेपाल सरकार
गृह मन्त्रालय

केदारबाबु शर्मा
सचिव