सूचनाको हकसम्बन्धी ऐन, २०६४ को दफा ५ तथा सूचनाको हकसम्बन्धी नियमावली, २०६५ को नियम ३ बमोजिम सार्वजनिक गरिएको

**(स्वतः प्रकाशन)**

# आर्थिक वर्ष ०८३/८४

## पहिलो त्रैमासिक (साउन- असोज)


नेपाल सरकार

प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय

सूचना प्रविधि तथा विद्युतीय शासन कार्यालय

**राष्ट्रिय साइबर सुरक्षा केन्द्र**

सिंहदरबार, काठमाडौं

फोनः०१-५७०५८४२, इमेलः info@ncsc.gov.np

# विषय सूची


१. केन्द्रको पृष्ठभूमिः ..... 3

२. केन्द्रको काम, कर्तव्य र अधिकारः ..... 3

३. निकायको स्वरूप र प्रकृतिः ..... 4

४. कार्यालयको संगठन संरचना, दरबन्दी तथा शाखाको कार्य विवरणः ..... 5

क) संगठन संरचनाः ..... 5

ख) दरबन्दी तेरिजः ..... 5

ग) कार्य विवरणः ..... 6

५. निकायबाट प्रदान गरिने सेवा ..... 12

६. सम्बद्ध ऐन, नियम, नीति, गठन आदेश तथा निर्देशिका, कार्यविधि र अन्य कानूनी व्यवस्थाः ..... 14

७. कार्यालयबाट सम्पादन भएका प्रमुख कार्यहरुः ..... 14

८. कार्यालयको वेबसाइटः www.ncsc.gov.np ..... 14

९. कार्यालयको ईमेलः info@ncsc.gov.np ..... 14

१०. कार्यालयको ठेगानाः सिंहदरबार, काठमाडौं ..... 14

११. आर्थिक कारोवार सम्बन्धी अद्यावधिक विवरणः ..... 14

१२. कार्यालय प्रमुख, प्रवक्ता, सूचना अधिकारी तथा गुनासो सुन्ने अधिकारीको नाम र सम्पर्क नम्बरः ..... 15

१३. प्रमाणीकरण गर्ने निकायको रुपमा कार्य गर्न इजाजत प्राप्त संस्था सम्बन्धी विवरणः ..... 15

## १. केन्द्रको पृष्ठभूमिः

राष्ट्रिय साइबर सुरक्षा नीति, २०८० मा रहेको व्यवस्था बमोजिम सूचना एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको सुरक्षा संस्थागत संरचनाहरु निर्माण एवम् सुदृढीकरण गर्ने कार्यका लागि साइबर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्द्धन, साइबर सुरक्षा सम्बन्धी पूर्वतयारी, रोकथाम, पहिचान र प्रतिकार्य गर्ने निकायको रुपमा कार्य गर्न, डिजिटल फरेन्सिक अनुसन्धान गर्न तथा साइबर सुरक्षासँग सम्बन्धित निकायको नियमनकारी निकायको रुपमा समेत कार्य गर्ने गरी मिति २०८०।१०।०९ गतेको नेपाल सरकार मन्त्रिपरिषद्को निर्णय अनुसार राष्ट्रिय साइबर सुरक्षा केन्द्र स्थापना भएको थियो।

यसैगरी, विद्युतीय माध्यमबाट हुने कारोबारलाई सुरक्षित, भरपर्दो र विश्वसनीय बनाउन विद्युतीय हस्ताक्षरको प्रयोगको व्यवस्थापन गर्ने मुख्य उद्देश्य सहित विद्युतीय कारोबार ऐन, २०६३ तथा विद्युतीय कारोवार नियमावली, २०६४ बमोजिम २०६४ पौष १९ गते प्रमाणीकरण नियन्त्रकको कार्यालयको स्थापना भएको थियो।

हाल नेपाल सरकार, मन्त्रिपरिषद्को मिति २०८३।०३।३२ को निर्णयानुसार प्रमाणीकरण नियन्त्रकको कार्यालय खारेज भएको र उक्त कर्यालयले साबिकमा गर्दै आएका सम्पूर्ण कार्यहरु समेत यस केन्द्रबाट सम्पादन भइरहेका छन्।

## २. केन्द्रको काम, कर्तव्य र अधिकारः

यस केन्द्रको काम, कर्तव्य र अधिकार देहाय बमोजिम रहेको छः-

- राष्ट्रिय साइबर सुरक्षा अवस्थाको अनुगमन तथा विश्लेषण गरी साइबर जोखिम तथा चुनौति (Threats) को पहिचान गर्ने।
- साइबर सुरक्षा एडभाइजरी (Cyber Security Advisory) लगायत आवश्यक सूचना प्रवाह गर्ने।
- सरकारी निकाय तथा सार्वजनिक डिजिटल प्रणाली र पूर्वाधारको साइबर सुरक्षा सुदृढीकरण गर्न आवश्यक प्राविधिक सहयोग, मार्गदर्शन तथा समन्वय गर्ने।
- साइबर सुरक्षा घटनाको पहिचान, वर्गीकरण, प्रतिक्रिया (Response), नियन्त्रण तथा पुनःस्थापनाका लागि राष्ट्रियस्तरको Incident Response तथा Coordination Mechanism सञ्चालन गर्ने।
- साइबर सुरक्षा घटनाको डिजिटल फोरेन्सिक तथा प्राविधिक अनुसन्धान गरी डिजिटल प्रमाणको संकलन, संरक्षण तथा विश्लेषणमा आवश्यक सहयोग गर्ने।
- सूचना प्रणाली तथा डिजिटल पूर्वाधारको साइबर सुरक्षा परीक्षण, Security Audit, Vulnerability Assessment and Penetration Testing (VAPT) तथा Risk Assessment सम्बन्धी कार्य सञ्चालन तथा समन्वय गर्ने।

- राष्ट्रिय साइबर सुरक्षा नीति, रणनीति, मापदण्ड, निर्देशिका, मार्गदर्शन तथा न्यूनतम सुरक्षा आवश्यकता (Minimum Security Requirements) तयारी गरी लागु गर्ने गराउने।
- Cyber Threat Intelligence तथा Cyber Threat Information Sharing का लागि राष्ट्रिय संयन्त्र तथा प्लाटफर्म विकास, सञ्चालन तथा समन्वय गर्ने।
- राष्ट्रिय Computer Emergency Response Team (CERT) सञ्चालन गरी सरकारी, सार्वजनिक, निजी र अन्य सरोकारवाला निकायबीच साइबर सुरक्षा सूचना आदान-प्रदान, समन्वय तथा सहकार्य गर्ने।
- साइबर सुरक्षा तथा विद्युतीय हस्ताक्षरसम्बन्धी क्षमता अभिवृद्धि तथा जनचेतनाका लागि तालिम तथा अन्य क्षमता विकास कार्यक्रम सञ्चालन गर्ने।
- राष्ट्रिय तथा अन्तर्राष्ट्रिय साइबर सुरक्षा सहकार्य विस्तार गर्दै साइबर जोखिम व्यवस्थापन, सूचना आदान-प्रदान, प्राविधिक सहयोग तथा राष्ट्रिय साइवर resilience अभिवृद्धिमा समन्वय गर्ने।
- प्रमाणीकरण गर्ने निकायको नियमनकारी निकायको रुपमा कार्य गर्ने।
- विद्युतीय माध्यमबाट हुने कारोवारलाई सुरक्षित, भरपर्दो र विश्वसनीय बनाउन विद्युतीय हस्ताक्षरको प्रयोगको व्यवस्थापन गर्ने।
- विद्युतीय हस्ताक्षर तथा Public Key Infrastructure (PKI) सँग सम्बन्धित नीति, मापदण्ड, निर्देशिका तथा कार्यविधि तयार गरी कार्यान्वयन गर्ने गराउने।
- विद्युतीय हस्ताक्षरको Root Certifying Authority (RCA) को Public Key Infrastructure (PKI) को सञ्चालन तथा व्यवस्थापन गर्ने।
- विद्युतीय कारोवार ऐन, २०६३ तथा नियमावली, २०६४ मा नियन्त्रकको काम कर्तव्य र अधिकार बमोजिम कार्य गर्ने।

## ३. निकायको स्वरूप र प्रकृतिः

यस केन्द्रको मुख्य कार्य नेपालमा साइबर सुरक्षा सुनिश्चित गर्नु तथा विद्युतीय हस्ताक्षर जारी गर्ने प्रमाणीकरण गर्ने निकाय (Certifying Authority (CA) हरूको नियामक निकायको रूपमा कार्य गर्नु रहेको छ।

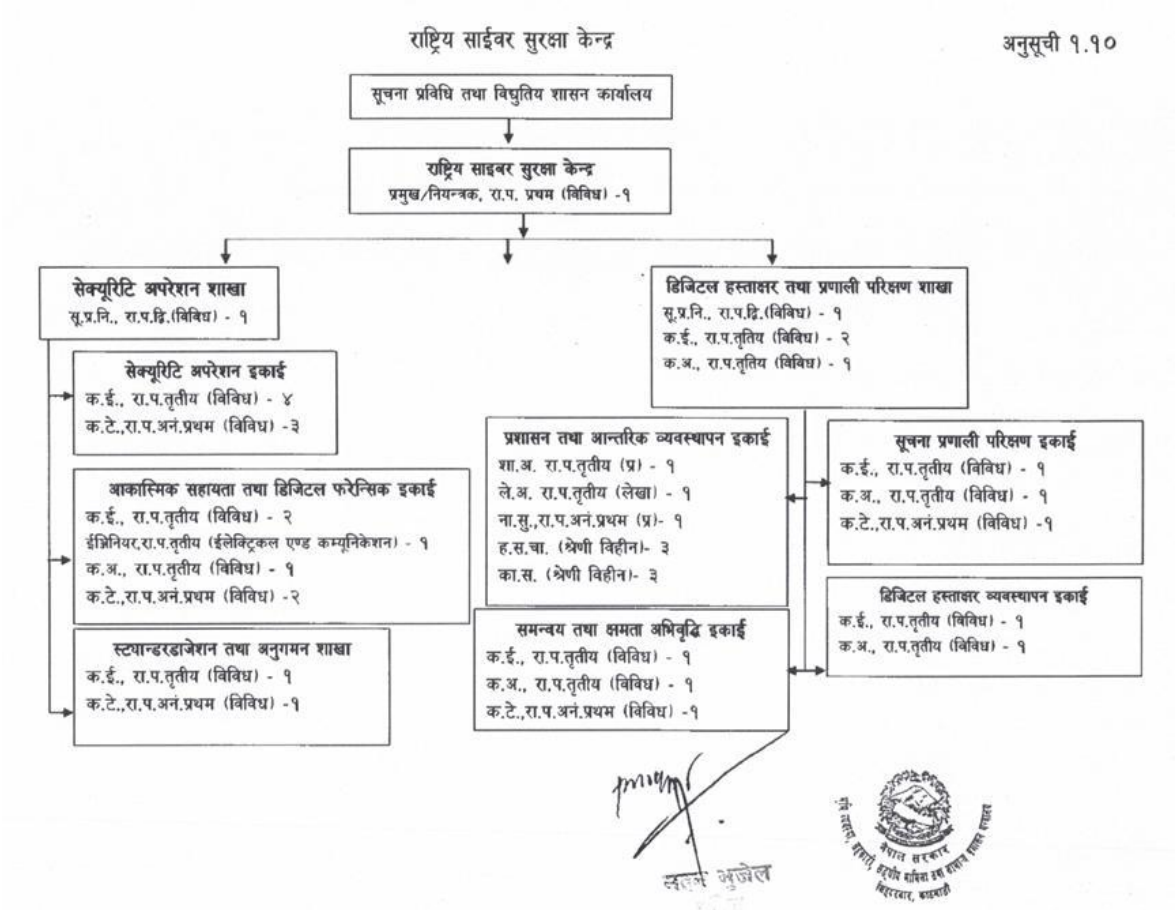
यस केन्द्रले नेपाल सरकारको साइबर सुरक्षा सम्बन्धी नीति, योजना, कार्यान्वयन तथा निगरानी गर्ने कार्य गर्दछ। साइबर हमलाबाट सरकारी प्रणाली, महत्वपूर्ण पूर्वाधार, नागरिक तथा निजी क्षेत्रलाई सुरक्षा प्रदान गर्ने, राष्ट्रिय नीति, निर्देशिका, कार्यविधि, तथा मापदण्ड तयार गर्ने, साइबर हमला वा अन्य साइबर घटनाबारे निगरानी गर्ने, विश्लेषण गर्ने र तत्काल प्रतिकार्य (Incident Response) दिने कार्य गर्ने, साथै साइबर सचेतना तथा प्राविधिक सहायता प्रदान गर्ने यस केन्द्रको उद्देश्य रहेको छ।

यसका साथै प्रमाणीकरण गर्ने निकायबाट विद्युतीय हस्ताक्षर जारी गर्ने कार्यको व्यवस्थापन गर्न यस केन्द्रले छुट्टै Public Key Infrastructure (PKI) पूर्वाधारको सञ्चालन समेत गर्दछ। प्रमाणीकरण गर्ने निकायले विद्युतीय कारोवार ऐन, नियमावली र इजाजतपत्र प्रदान गर्दा जारी गरेको शर्त बमोजिम कार्य गरे नगरेको सम्बन्धमा नियमित रुपमा अनुगमन गर्ने गर्दछ।

## ४. कार्यालयको संगठन संरचना, दरबन्दी तथा शाखाको कार्य विवरणः

### क) संगठन संरचनाः

यस केन्द्रको संगठन संरचना निम्न बमोजिम रहेको छः




### ख) दरबन्दी तेरिजः

कार्यालयको स्वीकृत दरबन्दी तेरिज निम्न बमोजिम रहेको छः

| क्र. सं. | पदनाम | श्रेणी/तह | सेवा | समूह | स्वीकृत दरबन्दी संख्या | पदपूर्ति संख्या | रिक्त संख्या | कैफियत |
|---|---|---|---|---|---|---|---|---|
| १ | प्रमुख/ नियन्त्रक | रा.प. प्रथम | नेपाल विविध | - | १ | १ | ० | |
| २ | सूचना प्रविधि निर्देशक | रा.प. द्वितीय | नेपाल विविध | - | २ | २ | ० | |
| ३ | कम्प्युटर इन्जिनियर | रा.प. तृतीय | नेपाल विविध | - | १० | ५ | ५ | |
| ४ | इलेक्ट्रोनिक इन्जिनियर | रा.प. तृतीय | नेपाल इन्जिनियरिङ्ग | इलेक्ट्रोनिक एन्ड टेलिकम्युनिकेसन | १ | ० | १ | |
| ५ | कम्प्युटर अधिकृत | रा.प. तृतीय | नेपाल विविध | - | ५ | ३ | २ | |
| ६ | शाखा अधिकृत | रा.प. तृतीय | नेपाल प्रशासन | सामान्य प्रशासन | १ | १ | ० | |
| ७ | लेखा अधिकृत | रा.प. तृतीय | नेपाल प्रशासन | लेखा | १ | १ | ० | |
| ८ | ना.सु. | रा.प.अनं. प्रथम | नेपाल प्रशासन | सामान्य प्रशासन | १ | १ | ० | |
| ९ | कम्प्युटर टेक्निसियन | रा.प.अनं. प्रथम | नेपाल विविध | - | ८ | ० | ८ | |
| १० | हलुका सवारी चालक | श्रेणी विहिन | - | - | ३ | २ | १ | |
| ११ | कार्यालय सहयोगी | श्रेणी विहिन | - | - | ३ | ३ | ० | |
| **जम्मा** | | | | | **३६** | **१९** | **१७** | |

**ग) कार्य विवरणः**

यस केन्द्रमा जम्मा दुइ वटा शाखा तथा शाखा अन्तर्गत जम्मा सात वटा इकाइहरु रहेका छन्। शाखा तथा इकाइहरुको कार्य विवरण देहाय बमोजिम रहेको छः

**<u>सेक्युरिटि अपरेशन शाखा</u>ः**

- केन्द्रको समग्र Security Operation, Cyber Incident Response तथा Digital Forensics सम्बन्धी कार्यको नेतृत्व, निर्देशन तथा समन्वय गर्ने।
- सरकारी निकाय तथा सार्वजनिक संस्थाका सूचना प्रणाली, नेटवर्क तथा डिजिटल पूर्वाधारको साइबर सुरक्षा अवस्थाको अनुगमन तथा विश्लेषण गर्ने व्यवस्था गर्ने।
- साइबर सुरक्षासँग सम्बन्धित नीति, मापदण्ड, निर्देशिका तथा कार्यविधिको मस्यौदा तयार गर्ने।
- विद्युतीय हस्ताक्षर तथा PKI सँग सम्बन्धित नीति, मापदण्ड, निर्देशिका तथा कार्यविधि तयार गर्ने।
- साइबर सुरक्षा घटना तथा जोखिमको पहिचान, वर्गीकरण, प्राथमिकता निर्धारण तथा आवश्यक प्रतिक्रिया व्यवस्थापन गर्ने।
- Cyber Threat Intelligence संकलन, विश्लेषण तथा आदान-प्रदानको समग्र व्यवस्थापन गर्ने।
- साइबर सुरक्षा घटना तथा जोखिम सम्बन्धी सूचना सम्बन्धित निकाय र सरोकारवालासँग समन्वय गर्ने।
- डिजिटल फरेन्सिक तथा घटना अनुसन्धान सम्बन्धी कार्यको समन्वय तथा गुणस्तर सुनिश्चित गर्ने।
- Cyber Incident Response, Digital Forensic तथा Security Operation सम्बन्धी कार्यविधी, Standard Operating Procedure (SOP) तथा प्रणाली विकास एवम् अद्यावधिक गर्ने।
- साइबर सुरक्षा अवस्था तथा घटना सम्बन्धी प्रतिवेदन तयार गर्ने।
- साइबर Exercise, Drill तथा अन्य आपतकालिन साइबर सुरक्षा अभ्यास सञ्चालनमा समन्वय गर्ने।

**<u>डिजिटल हस्ताक्षर तथा प्रणाली परिक्षण शाखाः</u>**

- डिजिटल हस्ताक्षर, सूचना प्रणाली परीक्षण, क्षमता अभिबृद्धि तथा प्रशासनिक व्यवस्थापन सम्बन्धी कार्यको नेतृत्व, निर्देशन तथा समन्वय गर्ने।
- विद्युतीय हस्ताक्षर र प्रमाणीकरण गर्ने निकाय सम्बन्धी नियमन तथा अनुगमन कार्यको समन्वय गर्ने।
- सूचना प्रणाली तथा पूर्वाधारको सुरक्षा परीक्षण (Security audit) तथा Compliance Assessment सम्बन्धी कार्यको समन्वय गर्ने।
- साइबर सुरक्षा तथा विद्युतीय हस्ताक्षर सम्बन्धी क्षमता अभिवृद्धि, जनचेतना तथा समन्वयका कार्यक्रम सञ्चालन गर्ने।
- राष्ट्रिय तथा अन्तर्राष्ट्रिय निकाय, CERT, सरकारी, निजी तथा प्राज्ञिक (Academia) क्षेत्रसँग आवश्यक समन्वय तथा सहकार्य गर्ने।
- केन्द्रको बार्षिक योजना तथा कार्यक्रम तर्जुमा तथा बजेट निर्माण गर्ने।
- शाखाअन्तर्गतका इकाईको कार्ययोजना तथा कार्यक्रम तयार गरी कार्यान्वयन तथा अनुगमन गर्ने।

- शाखासँग सम्बन्धित कार्यको प्रगति, समस्या तथा उपलब्धि सम्बन्धी प्रतिवेदन तयार गरी केन्द्र प्रमुखसमक्ष पेश गर्ने।
- शाखाअन्तर्गतका कार्यका लागि आवश्यक प्रणाली, कार्यविधि तथा समन्वय संयन्त्रको विकास तथा अद्यावधिक गर्ने।

**<u>सेक्युरिटि अपरेशन इकाइः</u>**

- सरकारी निकाय तथा सार्वजनिक संस्थाका सूचना प्रणाली, नेटवर्क तथा डिजिटल पूर्वाधारको नियमित तथा real-time सुरक्षा अनुगमन गर्ने।
- Security Operation Center (SOC) सञ्चालन गर्ने।
- सम्भावित साइबर आक्रमणको पहिचान गरी प्रारम्भिक विश्लेषण तथा वर्गीकरण गर्ने।
- Cyber Threat Intelligence तथा अन्य Threat Information संकलन, विश्लेषण, अभिलेखीकरण तथा सम्बन्धित निकायसँग आदान-प्रदान गर्ने।
- पहिचान भएका साइबर सुरक्षा घटनालाई गम्भीरता तथा प्रभावका आधारमा सम्बन्धित इकाई वा निकायमा Escalation गर्ने।
- साइबर सुरक्षा सम्बन्धी प्राविधिक समस्या समाधानका लागि आवश्यक सहायता उपलब्ध गराउने ।
- सुरक्षा अवस्था, Threat तथा Incident सम्बन्धी नियमित प्रतिवेदन तयार गर्ने।
- Cyber Threat Sharing Platform तथा Cyber Exercise/Drill को सञ्चालनमा आवश्यक प्राविधिक सहयोग गर्ने।
- केन्द्रको आन्तरिक नेटवर्क तथा सूचना पूर्वाधारको सुरक्षा अनुगमन, सचालन तथा आवश्यक प्राविधिक व्यवस्थापन गर्ने।

**<u>आकस्मिक सहायता तथा डिजिटल फरेन्सिक इकाइः</u>**

- Security Operation Center तथा अन्य निकायबाट प्राप्त साइबर सुरक्षा घटनामा आवश्यक Incident Response तथा प्राविधिक अनुसन्धान गर्ने।
- साइबर घटनाको Containment, Recovery तथा पुनःस्थापना गर्ने कार्यमा आवश्यक प्राविधिक सहयोग गर्ने।
- साइबर घटना सम्बन्धी सूचना, तथ्य तथा डिजिटल प्रमाणको संकलन, संरक्षण तथा विश्लेषण गर्ने।
- डिजिटल प्रमाणको Authenticity, Integrity तथा Chain of Custody कायम गर्ने।
- राष्ट्रिय तथा क्षेत्रगत कम्प्युटर आकस्मिक सहायता समूहसँग समन्वय तथा सहकार्य गर्ने।
- साइबर घटना (Cyber Incidence) को डिजिटल फरेन्सिक (Digital Forensic) Investigation गर्ने।
- डिजिटल फरेन्सिक प्रविधि तथा कार्यविधिको अध्ययन, प्रयोग तथा अद्यावधिक गर्ने।

- साइबर घटनाको कारण, प्रभाव तथा पुनरावृत्ति रोकथामका उपाय सम्वन्धी प्राविधिक प्रतिवेदन तथा सुझाव तयार गरी लागू गर्ने।
- अनुसन्धान तथा कानून कार्यान्वयन गर्ने निकायसँग समन्वय गर्ने।
- Cyber Incident Response Plan, Exercise तथा Drill को तयारी तथा सञ्चालनमा प्राविधिक सहयोग गर्ने।
- विद्युतीय हस्ताक्षर प्रयोग गरी कारोबार गर्दा भएको अपराध अनुसन्धानमा आवश्यक सहयोग तथा सहजीकरण गर्ने।

**<u>स्टयान्डरडाइजेशन तथा अनुगमन इकाइः</u>**

- साइबर सुरक्षा सम्बन्धी अल्पकालीन, मध्यकालीन तथा दीर्घकालीन नीति, रणनीति, योजना, निर्देशिका तथा मार्गदर्शनको मस्यौदा तयार गर्ने।
- विद्युतीय हस्ताक्षर तथा PKI सम्बन्धी नीति, मापदण्ड, निर्देशिका तथा कार्यविधिको मस्यौदा तयार गर्ने।
- सरकारी तथा सार्वजनिक निकायका सूचना प्रणाली तथा डिजिटल पूर्वाधारका लागि आवश्यक साइबर सुरक्षा मापदण्ड तथा Minimum Security Requirements तयार गर्ने।
- साइबर सुरक्षासम्बन्धी Standards, Indicators, Metrics तथा Maturity Assessment Framework विकास गर्ने।
- सार्वजनिक तथा निजी क्षेत्रबाट प्रदान गरिने साइबर सुरक्षा सेवाको आवश्यक गुणस्तर तथा मापदण्ड निर्धारण गर्ने।
- साइबर सुरक्षा Compliance तथा Risk Management सम्बन्धी Framework तथा अनुगमन प्रणाली विकास गर्ने।
- सरकारी तथा सार्वजनिक निकायमा साइबर सुरक्षा मापदण्ड तथा निर्देशिकाको कार्यान्वयन अवस्थाको अनुगमन गर्ने।
- Security Audit, Assessment तथा Incident Response बाट प्राप्त निष्कर्षका आधारमा साइबर सुरक्षा मापदण्ड तथा मार्गदर्शन अद्यावधिक गर्ने।
- राष्ट्रिय तथा अन्तर्राष्ट्रिय साइबर सुरक्षा Standards तथा Best Practices को अध्ययन गरी आवश्यक सुधार तथा परिमार्जन गर्ने।
- साइबर सुरक्षा अवस्थाको अनुगमनबाट प्राप्त विवरणको विश्लेषण गरी सुधारका लागि सुझाव तथा प्रतिवेदन तयार गर्ने।

**<u>सूचना प्रणाली परीक्षण इकाइः</u>**

- सूचना प्रणाली तथा डिजिटल पूर्वाधारको साइबर सुरक्षा Audit तथा Security Assessment को योजना तथा कार्यक्रम तयार गर्ने।
- सूचना प्रणाली, Application, Database, Network तथा Infrastructure का Security Controls परीक्षण गर्ने।
- VAPT तथा अन्य सुरक्षा नियन्त्रणको परीक्षण गर्ने।

- सूचना प्रणाली तथा पूर्वाधारमा रहेका कमजोरी तथा सम्भावित जोखिमको पहिचान र मूल्याङ्कन गर्ने।
- Cloud Security तथा Third-Party Service Provider को सुरक्षा व्यवस्था तथा अभ्यासको समीक्षा गर्ने।
- परीक्षणबाट प्राप्त निष्कर्षका आधारमा Risk तथा Priority सहित सुधारात्मक सुझाव दिने।
- Audit तथा Assessment प्रतिवेदन तयार गर्ने र सिफारिसको कार्यान्वयन अवस्थाको अनुगमन गर्ने।
- सूचना प्रणाली परीक्षण सम्वन्धी Methodology, Checklist तथा आवश्यक उपकरण/कार्यविधि विकास तथा अद्यावधिक गर्ने।

**<u>समन्वय तथा क्षमता अभिबृद्धि इकाइः</u>**

- केन्द्रको Website तथा आधिकारिक Digital Communication Platform को Content व्यवस्थापन गर्ने।
- क्षेत्रगत तथा प्रादेशिक रूपमा सञ्चालन हुने CERT को सूचीकरण तथा आवश्यक समन्वय गर्ने।
- आकस्मिक सहायता सम्बन्धी कार्यमा राष्ट्रिय तथा अन्तर्राष्ट्रिय समन्वय तथा सूचना आदान-प्रदानमा सहयोग गर्ने।
- सरकारी निकाय, विकास साझेदार, निजी क्षेत्र तथा राष्ट्रिय/क्षेत्रीय/अन्तर्राष्ट्रिय संस्थाबीच साइबर सुरक्षा सहकार्यका लागि समन्वय गर्ने।
- अन्तर्राष्ट्रिय तथा क्षेत्रीय CERT सञ्जालमा आवद्धता तथा सहकार्यको व्यवस्था मिलाउने ।
- साइबर सुरक्षासम्बन्धी Professional Certification तथा क्षमता अभिवृद्धिका कार्यक्रम सञ्चालन तथा समन्वय गर्ने।
- संघ, प्रदेश तथा स्थानीय तहका सरकारी कर्मचारी, निजी क्षेत्र तथा सर्वसाधारणका लागि साइबर सुरक्षा तालिम सामग्री विकास गर्ने।
- साइबर सुरक्षा, Data Privacy, विद्युतीय हस्ताक्षर तथा Cyber Hygiene सम्बन्धी जनचेतनामूलक सामग्री विकास तथा अभियान सञ्चालन गर्ने।
- तालिम तथा क्षमता अभिवृद्धि कार्यक्रमको आवश्यकता पहिचान, प्रभावकारिता मूल्याङ्कन तथा सुधार गर्ने।

**<u>प्रशासन तथा आन्तरिक व्यवस्थापन इकाइः</u>**

- केन्द्रको वार्षिक योजना तथा कार्यक्रम तर्जुमा तथा बजेट निर्माण गर्ने।
- केन्द्रको स्वीकृत कार्यक्रमको कार्यान्वयन, अनुगमन तथा प्रगति विवरण तयार गर्ने।
- केन्द्रबाट सञ्चालन हुने गोष्ठी, कार्यशाला, तालिम तथा अन्य कार्यक्रमको प्रशासनिक तथा व्यवस्थापकीय तयारी गर्ने।
- कर्मचारीको वैयक्तिक विवरण तथा प्रशासनिक अभिलेख व्यवस्थापन गर्ने।
- कर्मचारीको सरुवा, बढुवा, पदस्थापन, बिदा तथा अन्य सेवा सम्बन्धी प्रशासनिक कार्य गर्ने।
- जिन्सी, खरिद, सवारी साधन तथा सरकारी सम्पत्तिको व्यवस्थापन गर्ने।

- निकासा, खर्च, लेखा, फाँटवारी तथा आर्थिक विवरण सम्बन्धी कार्य गर्ने।
- राजस्व, धरौटी तथा बेरुजुको अभिलेख व्यवस्थापन तथा बेरुजु फछ्यौट सम्बन्धी कार्य गर्ने।
- केन्द्र प्रमुखलाई प्रशासनिक तथा आर्थिक विषयमा आवश्यक राय तथा सहयोग उपलब्ध गराउने
- केन्द्रको सामान्य प्रशासन तथा आर्थिक प्रशासन सम्बन्धी अन्य कार्य गर्ने।

**<u>डिजिटल हस्ताक्षर व्यवस्थापन इकाइ:</u>**

- विद्युतीय हस्ताक्षर तथा Public Key Infrastructure (PKI) सम्बन्धी प्रणाली तथा पूर्वाधारको सञ्चालन, व्यवस्थापन तथा सुरक्षा गर्ने।
- प्रमाणीकरण गर्ने निकायलाई इजाजतपत्र प्रदान, नवीकरण तथा मान्यता प्रदान सम्बन्धी कार्य गर्ने।
- प्रमाणीकरण गर्ने निकायको इजाजतपत्र निलम्बन तथा रद्द गर्ने।
- प्रमाणीकरण गर्ने निकायले आफ्नो कारोवार सञ्चालन गर्दा पालना गर्नु पर्ने शर्तहरु र ग्राहकसँग व्यवहार गर्दा अपनाउनु पर्ने प्रक्रिया निर्धारण गर्ने।
- प्रमाणीकरण गर्ने निकायको कार्यसम्पादन परीक्षण गर्नको लागि आवश्यकता अनुसार परीक्षकको नियुक्ति गर्ने र परीक्षकको काम कारवाहीको अनुगमन गर्ने।
- प्रमाणीकरण गर्ने निकायको काम कारवाही, प्राविधिक प्रणाली तथा सुरक्षा व्यवस्थाको नियमन, अनुगमन तथा मूल्याङ्कन गर्ने।
- प्रमाणीकरण गर्ने निकायले पालना गर्नुपर्ने प्राविधिक तथा सुरक्षा मापदण्ड, प्रक्रिया तथा शर्तको कार्यान्वयन अनुगमन गर्ने।
- Digital Certificate को ढाँचा, आवश्यक विवरण तथा प्रमाणपत्र सम्वन्धी प्राविधिक व्यवस्था निर्धारण गर्ने।
- प्रमाणीकरण गर्ने निकायको PKI Audit तथा VAPT लगायतका प्राविधिक परीक्षणमा सहजीकरण गर्ने।
- Certificate Revocation List (CRL) तथा National Repository को प्रकाशन, सञ्चालन, अद्यावधिक तथा व्यवस्थापन गर्ने।
- राष्ट्रिय PKI Network तथा System को सञ्चालन, सुरक्षा, Access Control, Backup तथा Recovery व्यवस्थापन गर्ने।
- प्रमाणीकरण गर्ने निकायहरूसँग PKI सम्बन्धी प्राविधिक समन्वय तथा Interoperability कायम गर्ने।
- PKI सम्बन्धी पूर्वाधार, उपकरण तथा प्रणालीको सुरक्षा, अभिलेख, जोखिम व्यवस्थापन तथा आवश्यक सुधार गर्ने।

## ५. निकायबाट प्रदान गरिने सेवा

यस केन्द्रबाट प्रदान गरिने सेवाहरु देहाय बमोजिम रहेका छन्:

| क्र. सं. | प्रदान गरिने सेवाहरू | पेश गर्नु पर्ने कागजातहरू | सेवा प्राप्त गर्न लाग्ने अवधि | लाग्ने दस्तुर | शाखा/इकाइ | जिम्मेवार अधिकारी र स्थान | उजुरी सुन्ने पदाधिकारी |
|---|---|---|---|---|---|---|---|
| १ | Security Operation बाट उपलब्ध हुने सेवाहरु | कार्यालय/संस्थाको आधिकारिक पत्र | १-२ हप्ता | निःशुल्क | सेक्युरिटि अपरेशन इकाइ | सम्बन्धित अधिकृत (सिंहदरबार स्थित कार्यालय) | प्रमुख/नियन्त्रक |
| २ | Vulnerability Assessment and Penetration Testing सम्बन्धी सेवा | कार्यालय/संस्थाको आधिकारिक पत्र तथा VAPT सम्बन्धी फारम | कार्य प्रकृति अनुसार | निःशुल्क | सूचना प्रणाली परीक्षण इकाइ | सम्बन्धित अधिकृत (अनामनगर स्थित कार्यालय) | प्रमुख/नियन्त्रक |
| ३ | Emergency Response सम्बन्धी सेवा | कार्यालय/संस्थाको आधिकारिक इमेल वा पत्र। | संवेदनशीलता अनुसार | निःशुल्क | आकस्मिक सहायता तथा डिजिटल फरेन्सिक इकाइ | सम्बन्धित अधिकृत (सिंहदरबार स्थित कार्यालय) | प्रमुख/नियन्त्रक |
| ४ | प्रमाणीकरण गर्ने निकायका रुपमा ईजाजतपत्र प्रदान गर्ने | विद्युतीय (इलेक्ट्रोनिक) कारोवार ऐन, २०६३ तथा विद्युतीय कारोवार नियमावली २०६४ मा उल्लेख भएबमोजिमका कागजातहरु | ६० दिन | २५,०००।- (पच्चीस हजार) | डिजिटल हस्ताक्षर व्यवस्थापन इकाइ | सम्बन्धित अधिकृत (अनामनगर स्थित कार्यालय) | प्रमुख/नियन्त्रक |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ५ | प्रमाणीकरण गर्ने निकायका रुपमा प्राप्त ईजाजतपत्रको नविकरण गर्ने | विद्युतीय (इलेक्ट्रोनिक) कारोवार ऐन, २०६३ तथा विद्युतीय कारोवार नियमावली २०६४ मा उल्लेख भएबमोजिमका कागजातहरु | निवेदन दर्ता मितिले १ महिना भित्र | २०,०००।- (बीस हजार मात्र) | डिजिटल हस्ताक्षर व्यवस्थापन इकाइ | सम्बन्धित अधिकृत (अनामनगर स्थित कार्यालय) | प्रमुख/नियन्त्रक |

## ६. सम्बद्ध ऐन, नियम, नीति, गठन आदेश तथा निर्देशिका, कार्यविधि र अन्य कानूनी व्यवस्थाः

यस केन्द्रसँग सम्बन्धित नीति तथा कानूनहरु निम्न बमोजिम रहेका छन्:

- राष्ट्रिय साइबर सुरक्षा नीति, २०८०
- विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३
- विद्युतीय कारोबार नियमावली, २०६४
- नेपाल सूचना प्रविधि आकस्मिक सहायता समूह सञ्चालन तथा व्यवस्थापन निर्देशिका, २०७५

## ७. कार्यालयबाट सम्पादन भएका प्रमुख कार्यहरुः

- विभिन्न निकायहरुका २० वटा सूचना प्रविधि प्रणालीहरुको Vulnerability Assessment and Penetration Testing (VAPT) सम्पन्न गरिएको।
- नेपाल सरकारको email प्रणाली र एकीकृत डाटा व्यवस्थापन केन्द्र (IDMC) मा रहेको VEEAM Backup Application गरी जम्मा २ वटा प्रणालीहरुलाई Security Information and Event Management (SIEM) Tool मा आवद्ध गरी निरन्तर रुपमा साइबर सुरक्षा अनुगमन गरिएको।
- विद्युतीय हस्ताक्षरसँग सम्बन्धित सूचना प्रविधि प्रणालीहरु नियमित रुपमा सञ्चालन गरिएको।
- विद्युतीय हस्ताक्षरको प्रमाणीकरण गर्ने निकायको नियमन गरिएको।
- राष्ट्रिय कम्प्यूटर आकस्मिक सहायता समूह (National CERT) सञ्चालन तथा व्यवस्थापन निर्देशिका, २०८३ को मस्यौदा तयार गरी स्वीकृतिको लागि सूचना प्रविधि तथा विद्युतीय शासन कार्यालयमा पेश गरिएको।

## ८. कार्यालयको वेबसाइटः www.ncsc.gov.np

## ९. कार्यालयको ईमेलः info@ncsc.gov.np

## १०. कार्यालयको ठेगानाः सिंहदरबार, काठमाडौं

## ११. आर्थिक कारोवार सम्बन्धी अद्यावधिक विवरणः

**वार्षिक विनियोजन र खर्चको विवरण** *(रु. हजारमा)*

| वार्षिक विनियोजीत बजेट | | | प्रथम त्रैमासिकसम्मको खर्च | | | वार्षिक विनियोजनमा खर्च प्रतिशत | | | कैफियत |
|---|---|---|---|---|---|---|---|---|---|
| पूँजीगत | चालु | जम्मा | पूँजीगत | चालु | जम्मा | पूँजीगत | चालु | जम्मा | |
| ३,९५,०० | ३,६९,२७ | ७,६४,२७ | ० | ५७,४८ | ५७,४८ | ० | १५.५७ | ७.५२ | |

प्रथम त्रैमासिकमा सङ्कलन भएको राजश्व एवम् आयको विवरण *(रु. हजारमा)*

| आम्दानीको शीर्षकको नाम | वार्षिक लक्ष्य (२०८३/८४) | प्रथम त्रैमासिकसम्म सङ्कलित रकम | प्रगति (प्रतिशत) |
|---|---|---|---|
| - | - | - | - |
| जम्मा | | - | - |

## १२. कार्यालय प्रमुख, प्रवक्ता, सूचना अधिकारी तथा गुनासो सुन्ने अधिकारीको नाम र सम्पर्क नम्बरः

- **कार्यालय प्रमुख** : श्री अनिल कुमार दत्त, ०१-५७०५२८२
- **प्रवक्ता** : सूचना प्रविधि निर्देशक श्री राज कुमार महर्जन, ९८५१४०२२८९
- **सूचना अधिकारी** : शाखा अधिकृत श्री अभय शेखर अधिकारी, ९७६३६९२२८९

## १३. प्रमाणीकरण गर्ने निकायको रुपमा कार्य गर्न इजाजत प्राप्त संस्था सम्बन्धी विवरणः

यस कार्यालयबाट मिति २०७१ साल मंसीर १ गते Radiant InfoTech Nepal Pvt. Ltd. ले प्रमाणीकरण गर्ने निकायको रुपमा इजाजत प्राप्त गरी विद्युतीय हस्ताक्षर प्रमाणपत्र जारी गर्दै आइरहेको छ।