(प्रशासन शाखा)

पत्र संख्या:- ९.१/२०७९/०८०/१९।२१
चलानी नं. १६९६

विषय:- सुरक्षा कार्यान्वयन सम्बन्धमा ।

मिति:- २०८०/०३/२७

श्री सर्व महाशाखा/शाखा, भूमि व्यवस्था, सहकारी तथा गरिबी निवारण मन्त्रालय ।
श्री राष्ट्रिय सहकारी विकास बोर्ड, पुल्चोक ।
श्री राष्ट्रिय भूमि आयोग, सिंहदरबार ।
श्री भूमि संरक्षण, प्रशासन कार्यालय सिन्धुपाल्चोक ।
श्री सहकारी व्यवसायका संस्थाको दर्ताकोठा, काठमाण्डौं ।
श्री भूमि व्यवस्थापन तथा अभिलेख विभाग, सम्पदापथ ।
श्री नगरी विकास मोलवास्थ ।
श्री सहकारी विभाग, सर्वसिद्धिका ।
श्री भूमि व्यवस्थापन प्रशिक्षण केन्द्र, सुनिचौर ।
श्री सहकारी सम्बन्धित उच्च अनुगमन केन्द्र, सर्वसिद्धिका ।
श्री राष्ट्र बैंकलगत सहकारी संस्था लि.पुल्चोक, ललितपुर ।
श्री राष्ट्र बचत तथा ऋण सहकारी संस्था लि. पुल्चोक, ललितपुर ।
श्री राष्ट्र सहकारी सहकारी संस्था लि, पुल्चोक, ललितपुर ।
श्री राष्ट्र सहकारी संस्था लि.काठमाडौं ।
श्री राष्ट्र स्वदेश प्रेम सहकारी संस्था लि. महाराजी कपन, चाबहील ।

प्रस्तुत विषयमा सम्बन्ध तथा सूचना प्रविधि मन्त्रालय तहबाट सुरक्षा सम्बन्धमा मिति ०७९/०८० च.नं. ०७९/०८० च.नं. सम्बु./१९९२ मिति २०८०/०३/०३ को पत्रको सूचिपत्रि पत्र ३ (दोष) मन्त्रालय सम्बन्ध छ । श्री मन्त्रालयमा "सूचना प्रविधि आकस्मिक सहायता समूह (समावर तथा व्यवस्थापन) नियमिका, २०७५" को दफा ३ बमोजिम राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह गठन भई नियमित रहेको व्यहोरा तथा उक्त सहायता समूहद्वारा समय-समयमा सुरक्षा सुरक्षामा देखिएका चुनौती (Threat) हरुको सम्बन्धमा Advisory हरु जारी गरिंदै । यसै क्रममा सुरक्षा चुनौती एवं जैविकतामा बढ्दो कमजोरी रोक्नको लागि उक्त आन्तरिक/बाह्य/विषय/संस्था तथा कर्मचारीका विभागहरुलाई आफ्ना सूचना प्रविधि प्रणालीलाई थप सुदृढ बनाउनका लागि उक्त आन्तरिक निर्देशन भएका सुझावहरु (Advisory) अनुसरण गर्न/गराउने व्यवस्थापन गरी मिति २०८०/०३/२७ को निर्णयानुसार अनुरोध छ ।

(सुदिप पौडेल)
सचिव

बोधार्थ:-
श्री सचिव तथा सूचना प्रविधि मन्त्रालय,
(साइबर सुरक्षा शाखा) सिंहदरबार ।
कम्प्युटर अभियन्ता श्री विष्णु बहादुर पौडेल:- Vishnu Pd Paudel

---

नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

साइबर सुरक्षा शाखा

सिंहदरबार, काठमाडौं

च.नं. :- ०७९/८०
च.नं. :- सञ्चु./२९९२

मिति :- २०८०/०३/२५

विषय: Cyber Hygiene सम्बन्धी Advisory।

श्री भूमि व्यवस्था, सहकारी तथा गरिबी निवारण मन्त्रालय , सिंहदरबार, काठमाडौं

प्रस्तुत विषयमा "सूचना प्रविधि आकस्मिक सहायता समूह (समावर तथा व्यवस्थापन) नियमिका, २०७५" को दफा ३ बमोजिम राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह गठन भई क्रियाशील रहेको व्यहोरा जानकारीको लागि अनुरोध छ। उक्त सहायता समूहद्वारा समय-समयमा साइबर सुरक्षामा देखिएका चुनौती (Threat) हरुको सम्बन्धमा Advisory हरु जारी गरिंदै। यसै क्रममा साइबर सुरक्षामा चुनौती एवं जैविकतामा बढ्दो कमजोरी रोक्नको लागि निजाय एवं बाह्यतका निकायलाई आफ्ना सूचना प्रविधि प्रणालीलाई थप सुदृढ बनाउनका लागि संलग्न कर्मचारीको सुझावहरु (Advisory) अनुसरण गर्न गराउने व्यवस्था हुन आदेशानुसार अनुरोध छ।

स्वप्निल किशोर कर्मचारी
डिजिटल हस्ताक्षर गरी मिति
Harkam Karki
harkama.karki@mail.gov.np

(हर्कम कर्की)
कम्प्युटर इन्जिनियर

Advisory

१। कर्मचारीहरु तथा कार्यालय प्रमुख तथा सम्पर्कमा आएका Email हरु Phishing तथा Spam email हुन सक्ने हुँदा त्यसको अधिकारिकता पुष्टि नगरेसम्म नखोल्ने। सधैं यस सम्बन्धमा आफ्ना कर्मचारीहरु तथा सरोकारवालाहरुलाई समेत सचेत गराउने।

२। बाह्य निकायमा प्रवेश भईरहेका सूचना प्रविधि प्रणाली, Email सेवाहरुमा अन्य प्रमाणीकरण सम्बन्ध माध्यम Multi-factor Authentication को प्रयोग गर्ने।

३। पासवर्ड राख्ने साथै लामो गर्न नसकिने गरी सुरक्षित Password (Non-Trivial Password Policy अनुसार) राख्ने ।

४। प्रयोगमा रहेका Anti-virus, Database, Application Libraries, Operating System, Network devices, Security devices, Servers आदिलाई नियमित रूपमा अद्यावधिक गर्ने।

५। सूचना प्रविधि प्रणालीहरुको विकास तथा प्रयोग गर्दा "नेपाल सरकारको सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) नियमिका, २०७१" ले तोकेका Government Enterprise Architecture (GEA) मापदण्डहरु पालना गर्ने।

६। नयाँ सूचना प्रविधि प्रणालीहरुको विकास गरी Live गर्नु अघि अनिवार्य रूपमा Vulnerability Assessment and Penetration Testing (VAPT) लगायतका सुरक्षा परीक्षण गर्ने।

७। सरकारी निकायहरुले विकास गरेका वा गर्न लगाइएका सूचना प्रविधि प्रणालीको Source Code सुरक्षित राख्ने अनिवार्य गर्ने व्यवस्था मिलाइने।

८। आ-आफ्ने निकायमा प्रवेश भईरहेका सूचना प्रविधि प्रणालीहरुको क्रमशः एक वर्षको एक पटक अनिवार्य रूपमा VAPT लगायतका सुरक्षा जाँच (Security Audit) गर्ने व्यवस्था मिलाइने।

नोट: सरकारी निकायहरुले VAPT वा लगि सूचना प्रविधि विज्ञहरुबाट सल्लाह लिन सक्नेछन्।

९। Application हरुमा SSL को प्रयोग गर्ने।

१०। Genuine License भएको hardware तथा software हरु मात्र प्रयोग गर्ने।

११। आफ्ने संस्थाको Business Continuity Plan तयार गरी राख्नु गर्ने। साथै डाटाको नियमित रूपमा Backup तथा Archive गरी सुरक्षित राख्ने।

१२। डाटाको Unauthorized प्रवेश हुन नदिन आफ्ने संस्थामा डाटा Encryption को व्यवस्था गर्ने।

१३। संस्थामा कार्यरत कर्मचारिहरुलाई साइबर सुरक्षासम्बन्धी नियम-निर्देशनहरु, चेतना, दिक्षा र क्षमताबृद्धि कोर्स नियमित प्रशिक्षण दिने।

१४। संस्थाले सूचना प्रविधिको प्रयोगमा आवश्यक Privacy Policy तथा Terms and Conditions निर्धारण गरी पालना गर्न निर्देशन दिने।

१५। संस्थाले कर्मचारिहरुलाई Personal डिभाइसहरुमा आधिकारिक डाटा संकेत गर्ने, share गर्ने वा प्रसारण गर्ने जस्ता कार्यलाई नियन्त्रणमा गर्ने।

१६। संस्थामा नरहेका वा छोडेका व्यक्ति/कर्मचारीको प्रयोगकर्ता खाताहरु (User Accounts) निष्क्रिय बनाउने। साथै क्रमबद्धरूप प्रयोग नभएका प्रयोगकर्ता खाताहरुलाई Deactivate गर्ने तथा खाता चालु गर्न अनुरोध आएमा मात्र Activate गर्ने ।

१७। साइबर सुरक्षाका उपकरणहरु (जस्तै Firewall, WAF, IPS/IDS) को प्रयोग गर्दा डिभाइसको उचित Configuration तथा Security Harden गरी मात्र प्रयोग गर्ने।

१८। नेटवर्कमा विशेष सुरक्षा सम्पादन गर्नका लागि Intrusion Detection/Prevention Systems (IDS/IPS) हरु प्रयोग गर्ने।

१९। Firewall मा Inbound र Outbound Rules हरु प्रयोग गरी कार्यालयभित्रको नेटवर्कलाई सुरक्षित बनाउने। यसै क्रममा Port हरु मात्र खुले, SSH/Telnet/RDP जस्ता Remote-Access Port हरुमा Brute-force माध्यम जोडिएर max-failed-trys-within-time-period परिभाषित गर्ने, आवश्यकता अनुसार IP Blocklisting / IP Whitelisting गर्ने, Port-Knocking को व्यवस्था गर्ने।

२०। वायरलेस नेटवर्कलाई आन्तरिक नेटवर्कबाट अलग गर्ने व्यवस्था मिलाइने। संस्थाका Application हरु Layer मार्फत पहुँच दीन बनाउने। Wi-Fi को प्रयोगलाई नियन्त्रणमा गर्ने तथा यसको प्रयोग Internet उपयोगको लागि मात्र गर्ने व्यवस्था मिलाइने।

२१। कार्यालयको Email ठेगाना व्यक्तिगत प्रयोजनको लागि प्रयोग नगर्ने।

२२। कुनै पनि सूचना प्रविधि सम्बन्धी उपकरणहरु मर्मतको लागि पठाउँदा सूचना चुहावट हुन सक्ने थाकाले डाटाका पहुँच नहुनेगरी (जस्त Hard disk, अन्य storage, memory) मर्मतको लागि पठाउने ।

२३। सूचना प्रविधि सम्बन्धी उपकरणहरुको मिलानि गर्दा Hard disk, Storage, Memory डिलिट मात्र मिलाउने। यसै जस्त Hard disk, अन्य Storage, Memory लाई भौतिक रूपमा पूर्ण नष्ट गर्ने ।

२४। साइबर आक्रमणका कुनै घटना भएमा वा कुनै संकास्पद ईमेल/लिङ्क/वाइरसहरु ईमेल मार्फत् प्राप्त भएमा सोको जानकारी राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूहको आधिकारिक वेबसाइट https://nitsah.gov.np मा गई रिपोर्ट गर्न सकिने।

Anil Kumar Dutta
Digitally signed by Anil Kumar Dutta
Date: 2023.07.07 14:43:43 +05'45'