नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

राष्ट्रिय साइबर सुरक्षा केन्द्र

सिंहदरबार, काठमाडौं

एडभाइजरी नं. NCSC-1146-113-01 मितिः २०८२/०७/१६

सूचना प्रविधि प्रणाली प्रयोगकर्ता तथा प्रणाली सञ्चालनकर्ता कर्मचारीहरुका लागि जारी गरिएको साइबर सुरक्षा एडभाइजरी

संघीय, प्रादेशिक तथा स्थानीय स्तरका सूचना प्रविधि प्रणालीका सर्वसाधारण प्रयोगकर्ताहरू र डाटाबेस/सिस्टम सञ्चालनकर्ताहरू (Administrators) लाई हालका साइबर जोखिमहरू, रोकथामका उपायहरू तथा सुरक्षित डिजिटल अभ्यासबारे सचेत बनाउने उद्देश्यले यो एडभाइजरी जारी गरिएको छ।

खण्ड कः साधारण प्रयोगकर्ताहरू (General Users):

यस खण्डमा दैनिक कार्यमा सूचना प्रविधि प्रणाली प्रयोग गर्ने साधारण प्रयोगकर्ताहरूका लागि निम्न अनुसारका आवश्यक सावधानी र सुरक्षित प्रयोगका उपायहरू समेटिएका छन्।

1. प्रत्येक एकाउन्टका लागि कम्तिमा १२ अक्षर लामो हुने गरी अंक, अक्षर र विशेष संकेतहरु सहितको फरक र जटिल पासवर्ड प्रयोग गर्नुहोस् तथा विश्वसनीय पासवर्ड म्यानेजर प्रयोग गरेर सुरक्षित रूपमा व्यवस्थापन गर्नुहोस् र पासवर्ड लाई नियमित (३-३ महिना वा आवश्यकता अनुसार) रूपमा परिवर्तन गर्नुहोस्।

2. सम्भव भएसम्म Multi-Factor Authentication (MFA) प्रयोग गरेर अतिरिक्त सुरक्षा तह थप्नुहोस्। यसका लागि भरपर्दो Authenticator एप्लिकेसन प्रयोग गर्नुहोस्।

3. प्रयोग सकिएपछि युजर एकाउन्टबाट वा वर्कस्टेशन (कम्प्युटर/ल्यापटप लगायत) बाट पूर्ण रूपमा लगआउट गर्नुहोस्। साथै सबै उपकरणमा Screen Lock PIN/Password/Pattern अनिवार्य गर्नुहोस्।

4. शंकास्पद इमेल, सन्देश वा फोनकलमा तुरुन्तै प्रतिक्रिया नगर्नुहोस्, अज्ञात लिङ्क वा Attachments मा क्लिक नगर्नुहोस् ; Password/One-Time Password (OTP) कसैसँग Share नगर्नुहोस्।

5. इमेल वा सन्देश प्रेषकको नाम, ठेगाना, समय जाँच गरेर मात्र खोल्नुहोस्; बैंक विवरण, नागरिकता नम्बर, पुरा ठेगाना जस्ता संवेदनशील जानकारी प्रेषक एकीन नगरी नपठाउनुहोस्।

6. "https://" बाट सुरु नभएको र ताल्चाको चिह्न (Padlock) नभएको साइटमा संवेदनशील जानकारी प्रविष्ट नगर्नुहोस्।

7. संवेदनशील कार्य वा वित्तीय कारोबार अपरिचित र सार्वजनिक Wi-Fi प्रयोग गरेर नगर्नुहोस्। आवश्यक परेमा सुरक्षित र भरपर्दो VPN अथवा मोबाइल डाटाको प्रयोग गर्नुहोस्।

8. सफ्टवेयर वा एप्स केवल आधिकारिक स्रोत (Google Play Store, Apple App Store, विक्रेताको आधिकारिक वेबसाइट) बाट मात्र डाउनलोड गर्नुहोस्।

9. अपरेटिङ सिस्टम (OS) र सबै एप्लिकेशनहरुमा नयाँ (Latest) सुरक्षा अपडेटहरू Install गर्नुहोस्; OS मा Antivirus Software Install गरेर Periodic Scan गर्नुहोस्।

10. बाह्य स्टोरेज उपकरण (जस्तै Pen Drive) प्रयोग गर्नु अघि भाइरस स्क्यान गर्नुहोस्; USB Auto-run Functionality निस्क्रिय गर्नुहोस्।

11. आफूले प्रयोग गर्ने एप्लिकेशनहरुलाई आवश्यक र सम्बन्धित Permission मात्र दिनुहोस्। (जस्तैः फोटो एडिट गर्ने एपलाई Location अनुमति, गेम एपलाई Contacts वा SMS अनुमति दिनु हुदैन।)

12. आफू वा सहकर्मीले प्रयोग गर्ने उपकरण वा प्रणालीमा असामान्य गतिविधि देखिएमा तुरुन्तै आफ्नो निकायको सुचना प्रविधि (IT) महाशाखा/शाखा/इकाई मा जानकारी गराउनुहोस्।

13. साइबर सुरक्षा सम्बन्धी प्रशिक्षण/जागरुकता कार्यक्रममा नियमित रूपमा सहभागी हुनुहोस्।

नोटः साइबर सुरक्षा सम्बन्धी विषयमा थप जानकारी वा सहयोग आवश्यक परेमा राष्ट्रिय साइबर सुरक्षा केन्द्र (NCSC) सँग समन्वय गर्नुहोस्।

सम्पर्कः info@ncsc.gov.np, टेलिफोनः ०१-४२११९३०, मो.नं.+९७७-९८५१४०२२८९(प्रवक्ता), +९७७-९७६३६९२२८९(सुचना अधिकारी)।

नेपाल सरकार
सञ्चार तथा सूचना प्रविधि मन्त्रालय
राष्ट्रिय साइबर सुरक्षा केन्द्र
सिंहदरबार, काठमाडौं

एडभाइजरी नं. NCSC-1146-113-01 मितिः २०८२/०७/१६

खण्ड खः डाटाबेस/सिस्टम सञ्चालनकर्ताहरू (System & Database Administrators):

यस खण्डमा सूचना प्रविधि प्रणालीको व्यवस्थापन, मर्मत तथा सुरक्षामा संलग्न डाटाबेस/सिस्टम सञ्चालनकर्ताहरूले सम्भव भएसम्म अपनाउनुपर्ने निम्न अनुसारका सुरक्षात्मक उपायहरू समेटिएका छन्।

1. सबै विशेषाधिकारयुक्त एकाउन्ट (जस्तैः admin) मा MFA अनिवार्य गर्नुहोस्, root Account लाई Disable गर्नुहोस् र SSH Public Key Authentication लाई प्राथमिकता दिनुहोस्। पासवर्ड/प्राइभेट की साधारण फाइल वा नोटप्याडमा नराखी सुरक्षित Vault को प्रयोग गर्नुहोस्।
2. Privileged Account मा Principle of Least Privilege लागू गर्नुहोस् साथै अनावश्यक Default Accounts (जस्तैः guest) Disable गर्नुहोस्।
3. Access को लागि Role-Based Access Control (RBAC) प्रयोग गर्नुहोस्।
4. Server, Workstation, Database मा नियमित Patch/Update लागू गर्नुहोस्, साथै सुरक्षित Latest Stable Version मात्र प्रयोग गर्नुहोस्।
5. Zero-Day Attack र Advanced Threats विरुद्ध Firewall, Intrusion Detection and Prevention System (IDPS), Endpoint Detection and Response (EDR), Sandboxing, Threat Intelligence जस्ता Defense-in-Depth Strategy अपनाउनुहोस्।
6. Router, Switch, Firewall जस्ता नेटवर्क उपकरणमा Default Credential (Username, Password) तुरुन्त परिवर्तन गर्नुहोस् र End-of-Life (EOL) / End-of-Service (EOS) निगरानी गर्नुहोस्।
7. Application र Database बीच Input Validation, SQL Injection Prevention र Development मा Secure Coding Practice लागू गर्नुहोस् साथै Security by Design Principle अवलम्बन गर्नुहोस्।
8. Remote Access का लागि VPN with Strong Encryption (IPSec/SSL VPN) मात्र प्रयोग गर्नुहोस्।
9. Network Segmentation र VLAN प्रयोग गरेर Demilitarized Zone (DMZ) स्थापना गरी External-facing Servers (Web, Mail, DNS) लाई आन्तरिक Network बाट अलग राख्नुहोस्।

10. आन्तरिक सरकारी सञ्चार र सेवाहरूको लागि प्रयोग हुने इन्ट्रानेट (Intranet) लाई सार्वजनिक र खुला इन्टरनेट (Internet) बाट अलग गर्नुहोस्।

11. सुचना प्रविधि प्रणाली र उपकरणमा देखिएका असामान्य गतिविधि (जस्तैः Failed Login, Port Scanning, DDoS Attack) का लागि Centralized Log Management System (SIEM Solution) मा आबद्ध गराई स्वचालित Alert/Monitoring को सेटअप गर्नुहोस्।

12. संवेदनशील डाटाको Encryption at Rest र Encryption in Transit दुवैमा Standard Encryption को प्रयोग अनिवार्य गर्नुहोस्।

13. ३-२-१ नियम (3 Copies of Data, 2 Different Media Types, 1 Off-Site Copy) अनुसार Backup राख्नुहोस् र Backup लाई पनि Encrypt गरेर सुरक्षित राख्नुहोस्। Backup Restore Testing Drill नियमित (कम्तिमा वार्षिक) रूपमा गर्नुहोस्।

14. Development/Testing Environment बाट Production Environment छुट्टै राख्नुहोस्।

15. डाटा सेन्टर, सर्भर कोठामा Physical Security को लागि सिसीटिभि, Sensor आदिबाट अनुगमन हुने व्यवस्था मिलाउनुहोस् र अधिकृत व्यक्तिलाई मात्र पहुँचको अनुमति दिनुहोस्।

16. निकायगत रुपमा प्रणाली सञ्चालनमा प्रयोगकर्ताले के के गर्ने, पासवर्डहरु कसरी राख्ने, उपकरणहरुमा पहुच, लगहरू सुरक्षित राख्ने अवधि, उपकरणहरु नष्ट गर्ने नीति (Policy for Password Management, Access Control, Log Retention, Device Disposal) बनाई लागू गर्नुहोस्।

17. एडमिनिस्ट्रेटर लेभलमा गरिएका संवेदनशील कार्यहरु आवश्यकता हेरी कार्यालय प्रमुखबाट प्रमाणित गरी अभिलेख राख्नुहोस् । (जस्तैः Backup Copy Off-site सार्नु वा Recovery Initiate गर्नु, Database मा Role/Privilege Grant/Revocation, Production Database को Full Export/Copy लिनु वा Restore गर्नु)

18. Post-Incident Analysis गरी Lessons Learned लाई अभिलेखीकृत गर्नुहोस्।

19. कम्तिमा वार्षिक रूपमा वा कुनै Function/Code परिवर्तन भएमा Vulnerability Assessment & Penetration Testing (VAPT) गर्नुहोस्।

नोटः साइबर सुरक्षा सम्बन्धी विषयमा थप जानकारी वा सहयोग आवश्यक परेमा राष्ट्रिय साइबर सुरक्षा केन्द्र (NCSC) सँग समन्वय गर्नुहोस्।

सम्पर्कः info@ncsc.gov.np, टेलिफोनः ०१-४२११९३०, मो.नं.+९७७-९८५१४०२२८९(प्रवक्ता), +९७७-९७६३६९२२८९(सुचना अधिकारी)।