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

मितिः २०८१/१०/०८

सरकारी सूचना प्रविधि प्रणालीको प्रयोगकर्ताका लागि जारी गरिएको साइबर सुरक्षा Advisory

क. सरकारी कार्यालयको Website, Application, Server , Storage तथा Network सुरक्षा सम्बन्धी

१. कार्यालयको वेबसाइटहरु नियमित रुपमा अपडेट गर्ने र समयानुकूल सुरक्षित Framework व्यवस्थापन गर्ने, साथै Website Security Audit गर्ने तथा देखिएका समस्यालाई तुरुन्त समाधान गर्ने,

२. आफ्नो निकायको Data को नियमित रुपमा Backup तथा Archive गर्नका साथै Business Continuity Plan तयार गरी लागू गर्ने,

३. Genuine License भएका Hardware तथा Software हरू मात्र प्रयोग गर्ने व्यवस्था मिलाउने,

४. कार्यालयमा प्रयोग भएका Anti-Virus, Database, Application Libraries, Operating System, Network Devices, Security Devices, Servers आदिलाई नियमित रुपमा Scan र Update/Patching गर्ने व्यवस्था मिलाउने,

५. आ-आफ्नो निकायमा प्रयोग भइराखेका साइवर सुरक्षाका उपकरणहरू (जस्तै Firewall, WAF, IPS/IDS) को प्रयोग गर्दा उचित Configuration तथा Security Harden गरी मात्र प्रयोग गर्ने,

६. Password राख्दा सहजै अनुमान गर्न नसकिने गरी सुरक्षित Password (Non-Trivial Password Policy अनुसार) राख्ने र तीन-तीन महिनामा परिवर्तन गर्नुपर्ने गरी प्रणालीमा व्यवस्था गर्ने,

७. नयाँ सूचना प्रविधि प्रणालीहरूको विकास गर्दा अनिवार्य रूपमा प्रत्येक चरणमा सुरक्षा परीक्षण गरेर मात्र प्रयोगमा ल्याउने,

८. आ-आफ्नो निकायमा प्रयोग भईरहेका सूचना प्रविधि प्रणालीहरुको कम्तीमा पनि वर्षको एक पटक अनिवार्य रूपमा सूरक्षा जाँच (Security Audit) गर्ने व्यवस्था मिलाउने र प्रणाली प्रयोग को Audit Log रहने व्यवस्था मिलाउने,

९. सरकारी निकायहरूद्वारा विकास गरिएका सूचना प्रविधि प्रणालीको Source Code अद्यावधिक गरी सुरक्षित राख्ने,

१०. आफ्नो निकायमा प्रयोग भईरहेका Email लगायतका सूचना प्रविधि प्रणालीहरुमा Multi-factor Authentication को प्रयोगलाई प्रोत्साहन गर्ने,

११. इमेल सुरक्षाको लागि Email Service Provider ले प्रदान गरेको Security Features लाई Enable गर्ने,

१२. व्यवस्थापन सूचना प्रणाली/पूर्वाधारमा' Need to Know' र' Least Privilege' को सिद्धान्त लागू गरी प्रयोगकर्तालाई आवश्यकताअनुसारको मात्र जानकारी र पहुँच प्रदान गर्ने व्यवस्था मिलाउने,

१३. अनावश्यक User Account हरुको निष्क्रिय गर्ने, अत्यावश्यक परेको बेला मात्र Root Account को सीमित प्रयोग गर्ने ,

१४. सर्भरको पहुँच र गतिविधिहरूको ट्रयाक गर्नको लागि सिस्टम लग र सर्भर लग Enable गर्ने र अनियमित गतिविधिहरूको निगरानी राख्ने,

१५. सम्भव भए सम्म Domain Controller/ Active Directory हरुको व्यवस्था गरी कार्यालयमा रहेका सबै कम्प्युटर उपकरणहरु लाई Centralized Management गर्ने व्यवस्था मिलाउने,

१६. कार्यालयका कम्प्युटरहरुमा आवश्यक USB पोर्टहरू मात्र Enable गर्ने र कार्यालयद्वारा प्रदान गरिएका वा स्वीकृत Removable उपकरणहरू मात्र कम्प्युटरहरुमा जोड्न मिल्ने गरी सुरक्षा को व्यवस्था मिलाउने,

१७. महत्त्वपूर्ण डेटा र सेवाहरूसँग सम्बन्धित सर्भर र अन्य नेटवर्क उपकरणहरूलाई सुरक्षित बनाउन नेटवर्क Segmentation लागू गर्ने,

१८. Website तथा Application हरुमा अनिवार्य रुपमा SSL Certificate install गर्ने व्यवस्था मिलाउने,

१९. संवेदनशील सूचना रहने क्षेत्र (Datacenter/ Server Room) हरुमा अनाधिकृत पहुँच हुन नदिनको लागि Access Control /Door Lock System को व्यवस्था मिलाउने,

२०. भौतिक सुरक्षाको लागि IP Camera सहितको Surveillance प्रणालीको जडान गरी अनुगमनको व्यवस्था मिलाउने,

२१. सूचना प्राविधि सम्बन्धी कार्य गर्ने सम्बन्धित कर्मचारीहरुको लागि नियमति रुपमा Data/ Application/ Network/ Cloud Security लगायतका साइबर सुरक्षा सम्बन्धी तालिम प्रदान गर्ने व्यवस्था मिलाउने

ख. कार्यालयमा रहेका डेस्कटप/ ल्यापटप र प्रिन्टर सुरक्षा सम्बन्धी

१. Genuine License भएका Operating System तथा Software हरू मात्र प्रयोग गर्ने, नियमित कार्यको लागि कम्प्युटर/ल्यापटप प्रयोग गर्दा केवल Standard प्रयोगकर्ता (Non Administrator) Account बाट मात्र प्रयोग गर्ने र सबै Account मा Strong Password सेट गर्ने,

२. Operating System र BIOS Firmware लाई नयाँ Update/Patch हरूलाई स्वचालित रूपमा विश्वसनीय स्रोतबाट अद्यावधिक हुनसक्ने गरी सेट गर्ने,

३. कम्प्युटर/ल्यापटपको Booting को लागि BIOS Password समेत सेट गर्ने,

४. कम्प्युटर/ल्यापटपमा Antivirus Client Install गरी सोलाई सबैभन्दा नयाँ Virus Definition, Signature र Patch हरूमा Upgrade गर्ने,

५. डेस्कटप/ ल्यापटप प्रयोग गर्नु नपर्ने अवस्थामा सधैं Lock/Logoff गर्ने तथा कार्यालय छोड्दा डेस्कटप/ल्यापटप लगायतका उपकरणहरुलाइ अनिवार्य रुपमा बन्द (Proper Shutdown) गर्ने,

६. डेस्कटप/ल्यापटप र मोबाइल फोनमा आवश्यक पर्दा बाहेक GPS, Bluetooth, NFC र अन्य Sensor हरूलाई Disabled राख्ने,

७. प्रिन्टरको सफ्टवेयरलाई Latest Available Version को Update/Patch हरूसँग अद्यावधिक गर्ने,

८. कार्यालयका Shared Printer हरू मा Unique Password सेट गर्ने साथै प्रिन्टरलाई इन्टरनेटको पहुँच नहुने गरी सेट गर्ने,

९. प्रिन्टरमा Print History भण्डारण गर्न निषेध गर्ने,

१०. USB, External Hard-Disk लगायतका Plug and Play Devices हरुको प्रयोग गर्दा हरेक पटक Security Scanning गरी सुरक्षित रहेको एकीन गरेर मात्र प्रयोग गर्ने,

११. डेटा सेन्टरमा रहेका ICT Infrastructure सँग Remote Access गर्न हार्डवेयर VPN/ Software VPN प्रयोग गर्ने,

१२. Password, IP address, Network Diagram वा अन्य संवेदनशील जानकारीलाई सम्बन्धित व्यक्ति बाहेक अरुले देख्ने/भेट्ने ठाउँमा नराख्ने,

१३. आन्तरिक सरकारी दस्तावेजहरूको Scanning का लागि Cam Scanner जस्ता कुनै पनि बाह्य मोबाइल एपमा आधारित Scanner सेवाको प्रयोग नगर्ने,

१४. Licensed सफ्टवेयरको सूचीमा नपर्ने कुनै पनि Pirated Operating System/ Software/Application को प्रयोग नगर्ने,

१५. अति आवश्यक परेको बेलामा मात्र सीमित समय र सीमित प्रयोगकर्ताका लागि मात्र File/ Folder Sharing गर्ने,

ग. Password व्यवस्थापन तथा सुरक्षा सम्बन्धी

१. Password राख्दा सहजै अनुमान गर्न नसकिने गरी ठूला र साना अक्षरहरू, संख्या, तथा विशेष चिन्हहरूको संयोजन भएको कम्तीमा ८ Character को सुरक्षित Password (Non-Trivial Password Policy बमोजिमको) राख्ने र प्रत्येक तीन-तीन महिनामा परिवर्तन गर्ने,
२. घर परिवारका आफन्त , साथीभाई आदिको नाम, मोबाईल नम्बर, फोन नं, ठेगाना, जन्म मिति जस्ता सजिलै अनुमान लगाउन सकिने शब्दहरु Password को रुपमा प्रयोग नगर्ने,
३. Password बनाउदा शब्दकोषमा भएका शब्दहरुको मात्र सँयोजन गरी नबनाउने,
४. संवेदनशील डाटा/सूचना रहने प्रणालीहरुमा पहुँचको लागि अनिवार्यरुपमा **Multi-Factor Authentication** को प्रयोग गर्ने,
५. एक भन्दा बढी सेवा, वेबसाइट तथा Applications (Digital Account) मा एउटै Password प्रयोग नगर्ने तथा पहिलानै प्रयोग भएको Password लाई पूनः प्रयोग नगर्ने,
६. कुनै पनि प्रणालीमा रहेको Default Password लाई तत्काल परिवर्तन गर्ने,
७. Password लाई अरु कसैलाई प्रदान नगरी गोप्य राख्ने र Password लाई सामाजिक सञ्जाल वा सञ्चार माध्यमबाट आदान प्रदान नगर्ने,
८. System Password, प्रिन्टर Password, वा Wi-Fi Password कुनै पनि अनधिकृत व्यक्तिलाई Share नगर्ने,
९. सम्भव भए सम्म Offline OTP Authenticator Application (जस्तै Google Authenticator) को प्रयोग गर्ने,

घ. Internet Browsing सुरक्षा सम्बन्धी

१. सरकारी Application/सेवाहरू, ईमेल सेवाहरू, बैंकिङ/भुक्तानी सम्बन्धित सेवा वा कुनै महत्त्वपूर्ण सेवा/Applications पहुँच गर्दा सधैं Private Browsing/Incognito Mode प्रयोग गर्ने,
२. User Login आवश्यक पर्ने साइटहरूमा Access गर्दा Link मा Click नगरी Browser को Address Bar मा साइटको Domain Name/URL Manually Type गर्ने,
३. इन्टरनेट Browser को नवीनतम संस्करण प्रयोग गर्ने र यसलाई नियमित रूपमा अद्यावधिक राख्ने,
४. Browser मा कुनै पनि Username र Password Save नगर्ने,
५. इन्टरनेट Browser मा कुनै पनि भुक्तानी सम्बन्धित जानकारी सुरक्षित नगर्ने,

६. Anonymous Third Party Services जस्तैः Nord VPN, Express VPN, Tor, Proxies आदिको प्रयोग नगर्ने,
७. Third party Tools तथा Gadgets जस्तैः Download Manager, Weather Toolbar, AskMe Toolbar आदिको प्रयोग नगर्ने,
८. अनधिकृत वा Pirated सामग्री जस्तैः Pirated फिल्महरू, गीतहरू, ई-बुक्स, सफ्टवेयर आदि डाउनलोड नगर्ने,
९. कार्यालयका कम्प्युटर/ल्यापटपमा कुनै पनि गेम Install गर्न वा खेल्न नखोज्ने,
१०. संक्षिप्त URL link हरू (जस्तैःtinyurl.com/ab534) खोल्दा Phishing/Malware Page हरुमा Redirect गर्न सक्ने हुदाँ सावधानी अपनाउने,

ङ. Email तथा Phishing Attack सुरक्षा सम्बन्धी

१. अपरिचित व्यक्ति तथा संस्थाबाट आएका Email हरु Phishing तथा Spam Email हुन सक्ने हुँदा त्यसको आधिकारिकता पुष्टि नभएसम्म नखोल्ने,
२. अपरिचित व्यक्ति वा ठेगानाबाट आएको शंकास्पद इमेलको File/Photo Attachment/Link लाई नखोल्ने,
३. अपरिचित व्यक्ति वा ठेगानाबाट आएको इमेल वा शंकास्पद इमेललाई तत्काल Spam Report गरी Delete गर्ने,
४. अत्यावश्यक बाहेकका Webpage/Newsletter/ Mailing List हरुमा Subscribe नगर्ने,
५. इमेल ,SMS, फोन मार्फत आफ्नो Password, OTP, Bank Account Number, PIN Code जस्ता विवरणहरु नपठाउने,
६. ईमेल खातामा Multi-Factor Authentication लाई Enabled गर्ने,
७. Business इमेल वा आफ्नो महत्वपूर्ण इमेल Public Hotspot/WiFi बाट नखोल्ने,
८. Remotely कम्पनीको इमेल खोल्दा Secured VPN को प्रयोग गरी सुरक्षित तवरले खोल्ने,
९. सार्वजनिक स्थानमा राखिएको कम्प्यूटरबाट इमेल Login गर्दा उक्त कम्प्यूटरमा भएको Keylogger को प्रयोग गरी Username तथा Password चोरी हुन सक्ने भएकोले त्यस्ता कम्प्यूटरबाट सकेसम्म login नगर्ने , गर्नैपर्ने अवस्थामा पनि On Screen Keyboard (OSK) को प्रयोग गर्ने,
१०. इमेल सुरक्षाको लागि Email Service Provider ले प्रदान गरेको Security Features लाई Enable गर्ने,

११. ईमेल सेवाको "Login History" Tab मा गएर विगतका Login गतिविधिहरू हेरी Login History मा कुनै Anomaly(असान्दर्भिक गतिविधि) देखिन्छ भने, तुरुन्तै सम्बन्धित निकायमा सम्पर्क गर्ने,

१२. प्राप्त हुन आएको कुनै इमेल वा वेबसाइटको विषयमा शंका लागेमा सम्बन्धित संस्थामा सम्पर्क गरी इमेल पठाउने व्यक्ति वा संस्थाको राम्रोसँग पहिचान गरेर मात्र Reply/Response गर्ने,

१३. औपचारिक संचारका लागि कुनै पनि अनधिकृत वा बाह्य ईमेल सेवा प्रयोग नगर्ने,

१४. महत्वपूर्ण जानकारीहरु जस्तै:- आर्थिक प्रतिवेदन/ Budget Details/Password/कर्मचारी विवरण आदि ईमेल मार्फत पठाउनै पर्ने हुदाँ ईमेललाई PGP (Pretty Good Privacy) वा Digital Certificate प्रयोग गरी Encrypt गरी पठाउने,

१५. पुरस्कार (Prize), उपहार (Gift), चिट्ठा (Lottery) लगायत बिभिन्न प्रलोभन देखाएर पठाईएको वा डर धम्की दिई पठाईएको इमेल, सन्देश, फोन कल लगायतलाई Reply/Response नगर्ने,

१६. Email मा PDF, TEXT, CSV जस्ता Standard Format बाहेकका exe, vbs जस्ता Extension का File हरु Click नगर्ने,

१७. आफूसँग सम्बन्धित नभएका Country Domain/Sub-Domain बाट आएका इमेलहरुलाई नखोल्ने,

१८. कुनै पनि वेबसाइटको राम्रोसँग पहिचान नगरी Login Credentials (User Name and Password), जन्ममिति, मोबाइल नम्बर, नागरिकता नम्बर लगायतका Personally Identifiable Information (PII) हरु Share नगर्ने,

१९. Macro function enabled भएका फाइलहरू डाउनलोड गर्दा वा खोल्दा सधैं "Disable Macros" विकल्प चयन गर्ने,

च. Removable Media सुरक्षा सम्बन्धी

१) Removable Media प्रयोग गर्नुअघि यसलाई Low Level Format गर्ने,

२) Removable Media का सामग्रीलाई सुरक्षित रूपमा मेटाउने,

३) Removable Media Access गर्नु अघि यसलाई Antivirus Software ले scan गर्ने,

४) Removable Media मा रहेका संवेदनशील फाइलहरू तथा फोल्डरहरू Encrypt गर्ने,

५) Removable Media मा रहने दस्तावेजहरूलाई Strong Password ले सुरक्षित गर्ने,

६) Removable Media लाई कुनै पनि अनधिकृत Devices मा Plugin नगर्ने,

७) Unauthorized or Unidentified Sources बाट प्राप्त Removable Media प्रयोग नगरी कार्यालयबाट प्रदान गरिएका वा स्वीकृत उपकरणहरू मात्र प्रयोग गर्ने,

छ. सामाजिक संजाल(Social Media) सुरक्षा सम्बन्धी

१) सामाजिक संजाल र Networking साइटहरूमा व्यक्तिगत जानकारीको प्रयोग र प्रचार सीमित र नियन्त्रित रुपमा मात्र गर्ने,

२) कुनै Friend Request/Follow Request/Chat Request स्वीकार गर्नु अघि व्यक्तिको Verification सधै जाँच गर्ने,

३) सामाजिक मिडिया खातामा Multi Factor Authentication Enable गर्ने,

४) कुनै पनि अनजान सम्पर्क वा प्रयोगकर्ताबाट पठाइएका लिंक वा फाइलमा Click नगर्ने

५) कुनै पनि प्रमाणित नभएका तथा आन्तरिक सरकारी जानकारी वा दस्तावेजलाई सामाजिक मिडियामा पोस्ट, प्रकाशित वा Share नगर्ने,

६) सरकारी Email Address हरु सामाजिक मिडिया Platform मा share नगर्ने,

ज. मोबाइल सुरक्षा सम्बन्धी

१) मोबाइल अपरेटिङ सिस्टमलाई पछिल्लो Update/Patch लागू गरी Secure गर्ने,

२) Wi-Fi, GPS, Bluetooth, NFC र अन्य Sensor हरू आवश्यकता अनुसार मात्र Enable गर्ने,

३) मोबाइल एपहरू विश्वसनीय स्रोतहरु Google Play Store (Android का लागि) र Apple App Store (iOS का लागि) बाट मात्र डाउनलोड गर्ने,

४) मोबाइल एप डाउनलोड गर्नु अघि एपको लोकप्रियता जाँच गर्ने र प्रयोगकर्ताहरूका समीक्षाहरू पढी Bad Reputation भएका वा नकारात्मक समीक्षा भएका एपहरू डाउनलोड गर्दा सावधानी अपनाउने,

५) कुनै पनि एप Install गर्नु अघि एपले मागेको Device Permission को उद्देश्यलाई ध्यानपूर्वक पढी/बुझीमात्र Access Allow गर्ने,

६) संवेदनशील छलफलमा सहभागी हुँदा मोबाइल फोन बन्द गर्ने वा सुरक्षित स्थानमा बाहिर राख्ने,

७) अज्ञात स्रोतबाट आएका Bluetooth Pairing वा File Sharing अनुरोधहरू स्वीकार नगर्ने,

८) कुनै पनि Application ले Permission माग्दा Application सँग सम्बन्धित Access Request मेल खाएको /नखाएको विश्लेषण गरी मात्र Access Approve गर्ने (जस्तै, Calculator App ले Phone Access माग्ने अवस्था),

९) फोनमा अनधिकृत पहुँच रोक्न Passcode/Security Pattern को प्रयोग गरी स्वतः Lock/Keypad Lock हुने व्यवस्था सक्रिय गर्ने,आफ्नो फोन र Internal/ External Memory Card को नियमित रूपमा Offline Backup गर्ने,

१०) कम्प्युटरबाट मोबाइलमा Data Transfer गर्नु अघि डाटालाई Latest Update भएको Antivirus Scan गर्ने,

११) SMS वा सामाजिक सञ्जालमार्फत साझा गरिएका आकर्षक Offer/छुट सम्बन्धी Link हरू खोल्दा सावधानी अपनाउने,

१२) आफ्नो फोनमा Automatic Download सुविधालाई निष्क्रिय राख्ने,

१३) आफ्नो फोनमा सधैं Latest Antivirus Security Solution स्थापित र सक्रिय राख्ने,

१४) मोबाइल हराएको वा चोरी भएको अवस्थामा उपयोगी हुन सक्ने उक्त उपकरणको १५-Digit को IMEI नम्बर Offline सुरक्षित राख्ने,

१५) मोबाइल फोन हराएमा Pre-selected नम्बरहरुमा Message आउने लगायतका सुविधासहितको Tracking Feature प्रयोग गर्ने,

नोटः साइबर सुरक्षा सम्बन्धी विषयमा केहि जिज्ञासा, जानकारी तथा सुझाव भएमा **info@ncsc.gov.np** वा राष्ट्रिय साइबर सुरक्षा केन्द्रको टेलिफोन नम्बरः **०१-४२१११९८**, मो.नं.+९७७-९८५१४०२२८९(प्रवक्ता), +९७७-९७६३६९२२८९(सूचना अधिकारी), मा सम्पर्क गर्नुहुन अनुरोध छ।