NEIGRIHMS

पूर्वोत्तर इंन्दिरा गांधी क्षेत्रीय स्वास्थ एवं आयुर्विज्ञान संस्थान शिलांग
NORTH EASTERN INDIRA GANDHI REGIONAL INSTITUTE OF HEALTH & MEDICAL SCIENCES, SHILLONG
(भारत सरकार स्वास्थ एवं परिवार कल्याण मंत्रालय स्वायत संस्थान)
(An Autonomous Institute, Ministry of Health and Family Welfare, Government of India)
निदेशक ब्लॉक मावडीयांगडीयांग, शिलांग - 793018 मेघालय
Director's Block, Mawdiangdiang, Shillong – 793018 Meghalaya

www.neigrihms.gov.in
EPABX : (0364) 2538025

NEIGR-IT/16/2023/ Dated 03/09/2024.

NOTICE

To maintain a secure and safe working environment, the latest Cyber Security guidelines issued by the Ministry of Health and Family Welfare is enclosed herewith for compliance. These guidelines are crucial for safeguarding our digital infrastructure and protecting sensitive information. Adhering to these guidelines is vital in protecting the Institute from cyber threats. All employees are therefore requested to ensure that they understand and follow these practices in their daily work activities.

(Lt. Cdr. Pawan Deep)
Deputy Director (Administration)

Memo No. NEIGR-IT/07/2023/Pt-I Dated 03/09/2024.

Copy to:

1. P.S to the Director, NEIGRIHMS for kind information of the Director, NEIGRIHMS.
2. All HOD/Section Head for kind information and to accordingly inform their staff for compliance.
3. All Notice Board.
4. Office copy.

(Lt. Cdr. Pawan Deep)
Deputy Director (Administration)

CYBER SECURITY GUIDELINES FOR OFFICIALS

DOs

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
2. Change your passwords at least once in 120 days.
3. Use multi-factor authentication, wherever available.
4. Save your data and files on the secondary drive (ex: d:\) and Maintain an offline backup of your critical data.
5. Ensure your system is updated with the latest patches/updates.
6. Ensure UEM (KACE) and EDR (SentinelOne) antivirus is installed.
7. Use authorized and licensed software only and Download genuine Apps from official sites.
8. When you leave your desk temporarily, always lock/log-off from your computer session.
9. **When you leave office, ensure that your computer and printers are properly shutdown and powered off.**
10. Keep the GPS, Bluetooth, Hotspots, NFC and other sensors disabled on your computers and mobile phones. Enable only when required.
11. Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
12. Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/ and bit.ly/3qab) and any links shared through SMS or social media, etc that are preceded by exciting offers/discounts, etc. Such links may lead to a phishing/malware webpage and compromise your device.
13. **Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in.**

DON'Ts

1. Don't use the same password in multiple services/websites/apps.
2. Don't save your passwords in the browser or in any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)
3. Don't save your data and files on the system drive (Ex: c:\ or root).
4. Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: google drive, dropbox, etc.).
5. Don't install or use any pirated software (ex: cracks, keygen, etc.).
6. Don't use obsolete or unsupported Operating Systems.
7. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
8. Don't open any links or attachments contained in the emails sent by any unknown sender.
9. Don't disclose any sensitive details on social media or 3rd party messaging apps.

Cyber Security Group, MoHFW