Detailed information may be obtained from https://www.cert-in.org.in

Cyber Security Dos and Don'ts

Cyber security of the institution is the shared responsibility of every officer and staff using office computer and connected to the hospital LAN network. The following are the Dos and Don'ts to be followed to prevent cyber-attack:

- **DO** install antivirus software provided by the institution, and update it on a regular basis as security alerts of viruses and worms. E scan antivirus has been procured by the institution and is mandatory to be installed in all office computer if the same is connected to NKN LAN internet line.
- **DO** enable the windows firewall from the control panel; it secures the local system from incoming & outgoing traffic. Never disable it.

- **DO** use hard-to-guess passwords or passphrases. A password should have a minimum of 10 characters using uppercase letters, lowercase letters, numbers and special characters.
- **DO** use different passwords for different accounts. If one password gets hacked, your other accounts are not compromised.
- **DO** keep your passwords or passphrases confidential. DON'T share them with others or write them down. You are responsible for all activities associated with your credentials.
- **DO** log out of any application especially E-Hospital modules before closing the browser.
- **DO** be vigilant for suspicious phising emails. In case od suspicion contact server room staff.
- **DO** beware of your surroundings when printing, copying, faxing or discussing sensitive information. Pick up information from printers, copiers or faxes in a timely manner.
- **DO** keep the computer password protected and lock your computer. This protects data from unauthorized access and use.
- **DO** report all security breach or any suspicious cyber incidents to server room staff at 4476 and Chairman e-Governance at chairmanegov@rmlh.nic.in

- **DON'T** use NKN line for public Wi-Fi hotspots. ONLY use LAN cable and officially provided virtual private network software to protect the data and the device.
- **DON'T** plug in unverified or unknown portable devices. These devices may be compromised with code and launch as soon as you plug them into a computer.
- **DON'T** leave sensitive information lying around the office. DON'T leave printouts or portable media containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorized disclosure.
- **DON'T** post any private or sensitive information, such as numbers, passwords or other private information, on public sites, including social media sites, and DON'T send it through email unless authorized to do so. Douse privacy settings on social media sites to restrict access to your personal information.
- **DON'T** open mail or attachments from an untrusted source. If you receive a suspicious email, the best thing to do is to delete the message, and report it to server room staff at 4476.
- **DON'T** click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks.
- **DON'T** download anything from sited you do not trust.

- **DON'T** install unauthorized programs on your work computer. Malicious applications often pose aslegitimate software. Contact your IT support staff to verify if an application may be installed.
- **DON'T** select "Remember My Password" option on login page.
- **DON'T** leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment.
- **DON'T** allow unauthorised person to use office computers, especially those having confidential data. Any such incident must be reported to hospital administration.

Dated 10.6.2021

Prof.(Dr) Sameek Bhattacharya
Chairman eGovernance

Copy to
MS office
All Addl MS
All departments and sections through HOD and I/C
DDA
Account officer
Dean ABVIMS
Registrar ABVIMS
COE ABVIMS
Dy Registrar
Dy COE ABVIMS
AO ABVIMS
Accounts Officer ABVIMS
Exe Engineer CPWD
Nursing Supdt