**F. No. Z.28105/138/2024-H-I [FTS- 8291608 ]**
**Government of India**
**Ministry of Health & Family Welfare**
**(Hospital-I Section)**

.....

Nirman Bhawan, New Delhi
Dated 14-08-2024

To

The Director,
Lady Hardinge Medical College & Associated Hospitals,
Shaheed Bhagat Singh Marg,
New Delhi-110001

The Medical Superintendent
Dr. RML Hospital
New Delhi-110001

The Medical Superintendent
Safdarjung Hospital
New Delhi -110029

**Subject: Cyber security guidelines for officials**

Sir/Madam,

I am directed to refer to the subject mentioned above and to forward herewith Cyber Security guidelines on Do's and Don'ts issued by Cyber Security Cell of this Ministry

2. It is requested to circulate these guidelines(copy enclosed) among all the staffs of the Hospitals for strict compliance.

3. An action taken report may also be shared with the Ministry.

Yours faithfully,

Signed by Abhishek Pandey
Date: 14-08-2024 11:15:04
(Abhishek Pandey)
Under Secretary to the Govt. of India
Tel. No. 011-23061510

Dr. Kabir Sardana
(Chairman E Governance)
14/08/2024

# 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***