IT - 15/6/2022-IT-HO-CPCB-HO

CPCB

Central Pollution Control Board

IT Division

Date: 05-Dec-2022

Cybersecurity Guidelines

To protect CPCB's network and computing infrastructure from emerging cyber-threats, all officials are requested to adhere to following cybersecurity guidelines:

1. **Personal Laptop:** No personal laptop is to be connected to CPCB's network as any unsecured system may compromise the security of entire network. In case any personal laptop is required to be connected to CPCB's network for official work, kindly contact the IT Division at Ext. No. 305.
2. **Online PDF Split:** Kindly do not upload PDFs containing official information to any online website for splitting. A visual guide has been uploaded by IT Division on KMS Portal ('Central Docs' Section) of E-Office about alternative ways of splitting PDFs.
3. **Pirated Software:** No official shall download or install any pirated software on the computer systems as they are illegal and can create a backdoor entry to the system through trojans etc.
4. **Email Services:** Use only NIC Email Services for all official communications.
5. **P2P Networks:** Kindly do not use the office network for accessing restricted P2P networks such as torrents etc.
6. **Antivirus Software:** Kindly ensure that anti-virus software provided by IT Division is installed on your system. In case it is not installed, kindly contact the IT Division at Ext. No. 490 for installation of anti-virus software.
7. **System Updates:** Kindly keep the automatic updates enabled on your Windows OS and do not defer the updates for later period.
8. **Passwords:** Kindly keep strong passwords, and change your computer and email passwords regularly.
9. **Suspicious Links/Shortened URLs:** Kindly do not click on any suspicious links or shortened URLs from untrusted source.
10. **VPN Services:** Kindly do not use any third-party VPN service through office network. Only NIC VPN to be used wherever needed.
11. **Personal WiFi Hotspot:** Kindly do not use personal WiFi Hotspot of your cellphone on a computer which is connected on CPCB LAN.
12. **External USB Storage:** Kindly minimize the use of USB based external storage solution such as Pen Drive, external HDD etc., as they may infect the computer and entire network. Instead, the Briefcase feature available on NIC Mail can be used for storing and sharing large files. A visual guide by NIC has been uploaded on KMS Portal ('Central Docs' Section) of E-Office on using Briefcase feature of NIC Email.

For any suspected cybersecurity breach, kindly inform immediately to Sh. Anurag Sharma, Scientist 'B', IT Division, at anurag.cpcb@gov.in or at Ext. No. 302.

(B. Vinod Babu)
Scientist 'F' & DH-IT

To:

1. DH-Building Division: For displaying the first page of guidelines on all the Notice Boards.

Copy to:

1. PA to CCB: For information of CCB, please.
2. AO to MS: For kind information of MS, please.

(B. Vinod Babu)
Scientist 'F' & DH-IT