

Dont's

- Don't let any unauthorized person use your computer system.
- Never select the "Remember my password" option.
- Don't share your password with anyone, not even your colleagues.
- Don't reveal the admin/root password to any unauthorized persons
- Do not connect your computer storing classified data to internet
- Don't allow staff to bring their own devices or software to run on the official computer.
- Don't use pirated or gifted copies of software as these may contain viruses and even facilitate intrusion into the system.
- Don't play computer games. These could be the main carriers of viruses for an intruder to break into your computer system.
- Don't store TOP SECRET or SECRET information permanently in the hard disk of PC. Whenever TOP SECRET or SECRET information is processed on the PC, erase the information immediately from the disk after the processing is over.
- Don't download free songs/videos or any objectionable material on PCs where official work is carried out as such downloads often contains malware.
- Do not use pen drivers/ USB data storage devices on official PCs.
- Do not use/ install freely available screen saver on internet as these may have encode spyware / Trojan.
- Don't be tricked into giving away confidential information.
- Don't use unprotected computer on public networks for carrying out official work.
- Don't leave sensitive information unattended on your desktop on official PCs
- Don't install unauthorised software programs on your office computer
- Don't post any private or sensitive information on any social media
- Don't open mail or attachment from an untrusted source. Report the same immediately as cyber attacker often trick you into visiting malicious sites and downloading malware to steal data& damage network.
- Never reply to emails requesting personal or financial information.