



Do's

Dont's

Do's

- Ensure physical security of computer / laptop and other IT assets.
- Ensure effective physical access control procedures by using multilevel passwords.
- Always use screen saver password, user login password and power on password.
- The password must be a complex one and hard to guess, change them every 15 days.
- The contents of CDs and flash drive are as good as written files. The external storage media containing classified data should be marked and treated like other classified documents.
- All classified documents must be stored in an encrypted form in PCs as well as external storage devices.
- In a multi user system, user log to be maintained.
- Before deleting the sensitive files, overwrite the files with some junk data to prevent restoration of sensitive data by any means or delete the data by using secure delete option.
- Avoid storing of files on desktop and C drive of the PC.

- Every new incoming storage media and software should be tested for malwares.
- Always use original software purchased from the authorized vendors.
- Use a standalone computer for internet work and no official work is to be permitted on that PC.
- Ensure proper marking of removable media like CD/DVD. The defective CD/DVD to be physically broken and destruction certificate for the same to be kept for auditing purpose.
- Always use UPS to ensure uninterrupted power supply and to prevent any corruption of data and software.

- Maintenance and rectification of PC faults to be undertaken in the presence of individual user. Under no circumstance the PC to be handed over to outside maintenance engineer alone.
- Ensure centralized printing of all documents. Network printer must be located in a secure place.
- Always keep the PC updated with antivirus and OS update patches
- Portable storage media used on internet machine to be scanned for spyware, Trojan viruses and other suspicious malware before being used on department LAN systems.
- Ensure first boot device is the internal HDD.
- Install latest software patches
- Install a personal firewall
- Never log in as Admin for day to day work.
- Take regular backups.
- Disable services that are not required.
- Always lock account while leaving the computer.
- Encrypt sensitive data on HDD.
- Wipe data from unused portion of the disk
- Local Security Policy:
 - (a) Show a customized warning screen
 - (b) Only have one Admin account.
 - (c) Set a strong Password policy.
 - (d) Set a strong Account lockout policy
 - (e) Disable file sharing
 - (f) Enable auditing
 - (g) Disable Guest account if not required
- Stay alert and report suspicious activity.
- Always use password protect for sensitive files and devices.
- Be cautious of suspicious e-mails and links.
- Delete information when it is no longer needed.
- Be aware of your surroundings when printing, copying, facing or discussing sensitive information.
- Physically secure your Laptop and never leave it unattended.