

DST/PIT/SecurityGuidelines-01/2006
Department of Science & Technology

Technology Bhavan
New Mehrauli Road
New Delhi – 110016.

Dated 8th January, 2007

Office Memorandum

Subject: IT SECURITY GUIDELINES

The Department has Local Area Network (LAN) which provides internet connectivity within the Technology Bhawan campus. Most of the officials specifically up to the level of Section Officer have been provided with latest desk top machines. Recently instances of theft of RAM fitted in the machines have taken place and hence **officers are requested to ensure that their systems are adequately protected.**

2. It has been observed that few personnel within DST are accessing websites which have objectionable content and are banned for access. These actions create danger of a virus attack in the network and few computers were recently found infected with virus which normally comes through such websites.

3. **Please note that record of websites visited from each machine is being maintained regularly.** Please ensure that your system has an access password to prevent such misuse. Such misuse makes the entire network of the department prone to virus attacks and network jam.

4. In view of the above, the broad **computer & its peripherals and internet user guidelines** as attached as Annexure may kindly be adhered. **PIT seeks your utmost cooperation in this regard.**

5. **Head of All Divisions are requested to identify a nodal officer** with whom necessary coordination can be done in taking a feedback on the above implementation and also to identify computers which carry classified or vital information.

(Milind Kulkarni)
Member-Secretary, PIT
Ph: 26590478
milind@nic.in

To,

All concerned.

IT SECURITY GUIDELINES

- Computers along with facilities like internet access, e-mail and storage facilities like pen drives, CDs and other information storage systems are intended to facilitate the official work and must be used for its intended purpose only. These systems should not be used for personal interest, hobbies and under any circumstances by use any way that may be disruptive, offensive or harmful to the government interest.
- Since network is regularly being monitored for the internet usage by the desktop of official, the official should ensure that only authorized users gets the access to the desktop issued in his/her name and no unauthorized person(s) has access to the desktop. In this regard, the entry to the use of desk top should be through a password. It is also advised that the password should be of at least 8 characters. In order to have a secure password, the password may be a combination of upper and lower case alphabets, numerals and special character to make it complex. The password should be changed at frequent intervals and should not be shared with any unauthorized persons particularly those visiting for maintaining the machine or removing the temporary files.
- The users are advised not to access game sites, unauthorized internet sites, chat sites and pornographic sites. Users should also refrain from using e-mail to propagate chain mails, propaganda e-mails and sending e-greetings particularly during the festive seasons since it jams the network. Similarly the users are not allowed to circulate electronic materials, internally within DST or externally to other individuals that can be in the disinterest of the Department or the Government of India.
- When a file or data containing classified or confidential information is being deleted, it still remains on the computer storage media like hard disk, floppy, CDs etc. This file can be recovered back using some special tools and therefore it is advisable to overwrite the file several times with junk data and then erase the file.
- Network is getting scanned for all the attachments that come through virus however e-mail users are advised to check all the attachments for authentic sender address before opening the file through Outlook Express. This can be done by visiting <mail.nic.in> and logging in to your account and checking the mail in 'INBOX' and 'Probably Spam' folders, since some wanted mail may be treated as Spam by the server. (for nay query please contact 478 or 401)
- Users are also advised to check CDs, pen drives, etc for virus before use. As far as possible use of floppy disks may be avoided since they are prone to virus attack easily.
- Back up of important data/ application software programme should be taken periodically (daily/weekly/monthly) depending on the volume of the data and size of the application. The back up data should be kept in safe custody and should not be used for any other purpose other than restoring the data from the back up mode. In case of classified and confidential information one set of back up may normally be kept at different geographical location to avoid its loss in accident.
- Lap tops/ Tablet PCs given to the officials are to facilitate their official work and should be brought to the office for official use on regular basis. Any such mobile systems taken for presentation should not carry any unauthorized/ confidential data or information and a proper record of its movement be maintained by the official. The system should be periodically checked for any virus particularly if it is being taken to another location for presentation or any other purpose.
- The pen drives issued to officials are being issued by name and they should be used solely for the official purpose.
- No personal pen/flash drive is to be used inside the office by the visitors/ employees.

- Any loss/ damage of pen drive issued for official purpose should immediately be reported to PIT and the officer should certify that the lost pen drive does not contain any classified or confidential data.

Apart from the above the following may kindly be perused:

- The user on a regular basis should visit the website <http://windowsupdate.microsoft.com> and update the machines with the latest patches released by Microsoft for any virus vulnerability.
- Users are advised not to change the settings of the IP address of their computers. In case of any confusion, the IP number should be confirmed from the NIC cell (ext. 401).
- No extra internet connection port be added without consulting Member Secretary, PIT (ext 478) or Scientist, NIC Cell (ext. 401).
- PIT may be kept informed by the administration before processing for acquiring any IT equipment or peripherals.
- Since we have an antivirus server installed on the LAN network, the NIC Cell may be informed to equip any new machines that is being installed or any machine which is formatted and reloaded for proper connectivity with Trend Micro AntiVirus Server.