

CONFIDENTIAL

**POLICY & COORDINATION DIVISION  
CENTRAL BUREAU OF INVESTIGATION**

**COMPUTER SECURITY GUIDELINES**

Version 1 (February 22, 2007)

<b>CHAPTER</b>	<b>CONTENTS</b>	<b>Page No.</b>
1.	<i>Introduction/Objective</i>	2-3
2.	<i>General</i>	4-9
3.	<i>Network Computers</i>	10 -12
4.	<i>INTERNET</i>	13 -14
5.	<i>Safe Custody/Record Keeping &amp; Disposal of Hardware</i>	15-16
6.	<i>CSO/Computer Security Audit</i>	17
7.	<i>DO's &amp; DON'Ts for Operator/User</i>	18 -20

## **CHAPTER-1**

### **INTRODUCTION**

#### **Introduction**

1.1 Recent developments in Information and Communication Technologies have provided unprecedented potential for extensive data storage, data mining, and data transfer. As computers are getting connected increasingly through Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN) and INTERNET, the ease and the speed with which information is stored, retrieved or transmitted have thrown up wide range of vulnerabilities, which are highly dynamic and complex. The most secure computers are those which are not connected to the Network or INTERNET and shielded from any interference.

1.2 Local Area Network (LAN), Wide Area Network (WAN) and Metropolitan Area Network (MAN) as such are vulnerable to Interception, Compromise, Contamination, Denial of Information/ Service attacks etc. The vulnerability increases manifold, when the Network is connected to the INTERNET. Computer Networks follow Open-System Computer Architecture and Standard Communication Protocols. These Hardware Interfaces and Communication Protocols are openly known and available. And unless secured by an appropriately designed Computer Security Regimen/Protocol, the Data/Information in the Network can not only be surreptitiously/passively intercepted, but also be actively modified or destroyed. Denial of Service Attacks (DoS)<sup>1</sup> has become common by injecting malicious codes. Trojan Horse<sup>2</sup> and Spyware<sup>3</sup> Software could be embedded in the system through e-mail or contaminated computer media.

1.3 Some of the Computer and Network vulnerabilities that have been noticed in a number of organisations in recent days are:

- Physical thefts of Hard Disks, Computer Storage Media (CSM<sup>4</sup>), Keyboards with memory facility, used Printer Cartridges, Laptops etc.
- Stealing/compromising Data/Information by Remote Access.
- Accidental/Intentional cross connection between the Organisation LAN, WAN, MAN and INTERNET.

---

<sup>1</sup> **DoS:** Attempt to make service unavailable to the legitimate user; generally by flooding with meaningless data or sending information that causes the service to crash.

<sup>2</sup> **Trojan Horse:** A software program that appears to perform a valid function but that contains, hidden in its code, instructions that cause severe damage to the system. Unlike Viruses, it cannot replicate itself.

<sup>3</sup> **Spyware:** A software program hidden in a system to collect information stealthily.

<sup>4</sup> **CSM:** Hard Disk, Floppy; CD, DVD, Cartridge Tape, DAT, ZIP Disk, Pen Drive, SD Cards etc.

- Spoofing by Intruders.
- Defacing of various Web-sites by anonymous Hackers.

1.4 Threats to the Computer Security could emanate from Internal Sources such as subverted/disgruntled employees, as well as from External Sources such as the vendors of the Hardware/ Software, outsider Maintenance Staff or from intruders/hackers in the Cyber Space. Threats can manifest as Structured (automated methods of information gathering and attack - organized, determined and goal centric) or Unstructured (network loitering, manual information gathering or attack and misuse by accident).

### **Objective**

1.5 The main areas of Computer Security are:

- Access Control
- Confidentiality -denial of access to unauthorised personal Pen/Flash Drive etc.
- Data Loss/Theft
- Integrity -protection against unauthorised changes
- Authentication -establishing the identity of the actual user

1.6 The objective of these Guidelines is to help the Computer Administrators, Custodians, Users and Operators, to evolve and follow well defined procedures for safeguarding the computer Hardware, Software and the Data/Information stored and transacted in the Stand-Alone Computer or the Computer Network. The Guidelines are aimed at creating a secure system and providing for Defence in Depth, without compromising on the Primary Functionalities of the Computers/ Computer Network.

## **CHAPTER -2**

### **GENERAL**

2.1 The Computer Security Programme can be broken down into following specific stages:

- **Security Risk Analysis**

Systems Division will carry out analysis of the security threat / vulnerability from time to time for computer systems and accordingly draw/ revise a plan for Security Policy/ Guidelines for the officers and staff to follow. In case of necessity, System Division may take help of an expert.

- **Adoption of a Security Policy**

Policy Division shall issue well defined/ documented Security Policy or amendments to the existing guidelines, on basis of which appropriate guidelines for officers and staff should be issued by the branch SsP.

- **Development of an Information Classification System**

The classification should be done in basis of Para 2.1 - 2.4(3-5) and 3 of MHA Manual of Departmental Security Instructions.

- **Implementation of the Security Standard Manual**

Security Standards issued by CERT-In (Department of Information Technology) should be followed.

- **Ongoing Security Programme Updating / Enforcement**

As the Computer/Information technology is ever evolving, the Security Policy needs to be continuously reviewed and updated. The Systems Division would discharge this responsibility and based on its input the Policy Division would issue fresh/ amended guidelines from time to time.

- **Training and Periodic Briefing**

To remain familiarised with the evolving computer vulnerabilities /threats and protective measures, there should be periodic training and briefing of the

officers and staff. The Systems Division would coordinate such trainings with CBI Academy.

### **Physical Security**

2.2 Adequate physical security procedures/measures should be in place against theft, destruction/damage by fire or natural calamities, environmental damage and access by unauthorised persons.

2.3 The contents of a **CSM** are as good as written files. Therefore, all protective security measures and instructions as laid down in the MHA Manual of Departmental Security Instructions, *mutatis mutandis*, should apply for **use, custody, storage and transport** of such media.

2.4 The **CSM** should be transported in safe/sealed mailboxes to prevent damages.

### **Installation/Maintenance**

2.5 While installing the Operating System (OS), only the **Utilities/Components** required by the user should be installed/ enabled. Some of the Utilities listed below, which are enabled by default with the bundled Software must either be disabled or configured on need basis.

- Default Password
- Sample networking programme
- File sharing tools
- Ports enabled by default

2.6 The in-house maintenance capability may be nurtured, if possible, to reduce vulnerability of the system during maintenance by outside agencies.

2.7 Maintenance or rectification of faults in the computer system should be carried out under proper and close supervision. In case of maintenance of Hardware/Software by an external agency, a responsible computer knowing officer should invariably be present throughout the maintenance. It should be ensured that no data-file/program is copied and taken by the outsider Maintenance Engineer.

2.8 The maintenance of Software is often done by Vendors and as such it may be ensured that when the vendor/his representative is carrying out the maintenance work on the software, a responsible computer knowing personnel is present along with the engineer. It may also be ensured that the vendor does not get access to any sensitive data/information of the organisation. The vendors can at best be permitted to create some dummy files purely for maintenance purpose.

2.9 Whenever, the outsider Maintenance Engineer is allowed to install his own keyboards and other accessories as an interim measure till repaired part is returned, it may be ensured that his accessory may not have data capturing tools like key logger installed.

2.10 CSM should be kept away from any kind of magnetic field producers like speakers, batteries, monitor, etc.

2.11 Uninterrupted Power Supply (UPS) should be used to prevent corruption of Data and Software due to sudden power fluctuations/failure. Proper grounding of the power supply and system should be ensured. ,

### **Password**

2.12 Every computer/terminal should be protected with Multilevel (BIOS/OS/Application level) Passwords<sup>5</sup>. Each level should have different password.

2.13 A Password should have at least 8 characters and be a combination of upper and lower case alphabets, numerals and special characters to make it complex.

2.14 Passwords should be changed periodically, at least once in a fortnight, and must not be shared with any unauthorised person.

2.15 Apply the following tests to create strong password:

- Strong test: Is the Password as strong (in length and content) as the rules prescribe?
- Unique test: Is the Password unique and unrelated to your profile or other Passwords?
- Practical test: Can you remember it without having to write it down?
- Recent test: Have you changed it recently as prescribed?

### **Access Control**

2.16 Computers used for Classified Application<sup>6</sup> should have additional level of Security by installing effective Biometric Access Control (BAC) System.

2.17 When a computer is used as Stand Alone for confidential/ sensitive work, it may not be provided with the Network and Communication Ports.

---

<sup>5</sup> **Password:** An arbitrary string of characters chosen by a user or (system administrator) and used to authenticate the user when he attempts to log on, in order to prevent unauthorised access to his account.

<sup>6</sup> Classified Applications include creating, storing, transmitting classified Data and Information.

2.18 Appropriate Software tools like Device Lock may be installed to disable USB Ports, Parallel Ports, Communication Ports, Floppy Drives and other removable Drives. Such Ports/Drives may be enabled by the authorised user only when required. Soon after the requirement is met, the Ports/Drives should be disabled. Record of such activity should be maintained.

2.19 As a general rule, no computer utilised for Classified Application should be provided with internal Combo Drives (*CD/DVD* Reader plus CD writer or *CD/DVD* Writer). Only external J combo drives/*CD* writer/*DVD* Writer should be used on need basis, on specific authorisation by the Controlling Officer in writing. Such drives should be kept in safe custody under lock and key, when not used.

2.20 Wherever necessary, Hardware/Software security locks should be procured and installed as a protection against unauthorised access. If Hardware security lock is not available and the computer is used for storing extremely sensitive classified data, it may be kept in a protective case having lock and key.

2.21 As many free and paid on-line storage facilities are available on Internet, care must be taken to ensure that no one uses such facilities to transfer and store sensitive/ confidential information.

### **Detecting unauthorised Access**

2.22 Audit- Trail/System-Event-Log features and other Intrusion Detection System (IDS) should be enabled and checked regularly to find out any unusual/doubtful activity or breach of security. Every unusual activity or breach of security noticed by the user should be reported to the Controlling Officer immediately.

2.23 The Real Time Clock (RTC) of the Computer should be set accurately to ensure the accuracy of the audit-locks, which may be required for analysing breach of security.

2.24 The RTC of the Computer or Communication Device should be set to Indian Standard Time (1ST). There should be a procedure to check and correct drift in the RTC.

### **Safe Storage of Classified/Sensitive Data**

2.25 A suitable encryption package for storing Top Secret / Highly Sensitive Data in CSM may be identified and used, as necessary.

2.26 The removable Hard Disk and the Computer Media containing encryption/decryption algorithm, if being used, should be kept at a highly secured place, as applicable to paper based files of similar classification. The source keys/program for encryption/decryption should be kept in a separate media and cabinet.

2.27 Copying of data from the CSM should be done under proper authorisation by the Controlling Officer<sup>7</sup>.

2.28 When a file is deleted, its contents 'are not actually erased from the CSM. With appropriate tools the contents can be retrieved. To reduce this security risk, the file contains classified data may be overwritten several times (minimum 7 times) with the Junk Data.

2.29 CSM with Read only facility like CDR/DVDR, used for Classified work should be kept in safe custody. It is recommended to destroy those, when not required, by following set procedures.

### **Preventing Data Corruption/Loss**

2.30 Back Up of Data/ Application Software Programs should be taken periodically, daily/weekly depending on volume of data and nature of application, and kept in safe custody under lock and key for avoiding loss due to unforeseen causes including Virus attacks.

2.31 To avoid contamination, the Back Up media should not be used for any purpose other than updating the backup or restoring data. Drives available for taking backup/restoration should be enabled at the time of taking/restoring Back Up only, by the Authorised Officer<sup>8</sup>. These Drives must be disabled immediately after the Back Up/ restoration operation is complete.

2.32 Keeping one set of Back Up containing classified/sensitive data at a geographically different location may be implemented as far as possible.

### **Measures against Virus Infection**

2.33 Use of Pirated and unauthorised Software is strictly prohibited. Only the original licensed Software with high Virus-Resistant/Virus-Proof rating should be procured from the authorised vendors.

2.34 All computers should be installed with the latest Anti-Virus and Internet Security Software. Anti-Virus Programme looks for a typical Virus Signature and thwart/eliminate Viruses and other malicious Software (Malware). Internet

---

<sup>7</sup> **Controlling Officer:** A supervisory officer in charge of the section/branch/unit, and of and above the rank of DySP and equivalent.

<sup>8</sup> **Authorised Officer:** An officer authorised by the controlling officer/competent authority

security software prevents downloading of spam and other dangerous data stealing software.

2.35 Regular upgrading/updates to protect vulnerability against new Viruses should be ensured.

2.36 Data brought in a CSM should be checked first for presence of Virus and cured before use.

2.37 Application programs and tools in Disks/Cartridge Tapes/Re-Writable CDs/DVDs and other data storage devices like pen drives/ SD cards should not be loaned out as these may be returned with Virus. If, however, it becomes unavoidable, only a copy in a CD-R/ DVD-R and not the original be given.

### **Laptop/Pen Drive**

2.38 Disable the Bluetooth/WiFi features in official Laptop.

2.39 No personal Laptop/Palmtop/Electronic Note Book and Mobile Phones with Blue Tooth/GPRS should be permitted to be brought into the office by the visitors.

2.40 In case a Laptop/Palmtop/Electronic Note Book is required to be brought inside for specific purpose, the Bluetooth/WiFi feature, if present, should be disabled and the user/owner should be escorted till his exit to prevent any enabling during the visit.

2.41 Any Laptop taken out for presentation should be checked by the Controlling Officer for containing any unauthorised data/ information. On return, it should be checked for any Virus. Proper record of transport of data through Laptop should be kept.

2.42 No Personal Pen/Flash Drive should be permitted inside the office by the visitors/employees.

2.43 Official Pen Drive should be issued to the officer by name, as and when required, by the Competent Authority<sup>9</sup>, It should not be taken out of the office except under the circumstances/ conditions noted at para 2.41 above.

### **Miscellaneous**

2.4 Security Guidelines (CISG -2003-01) issued by CERT-IN for Stand Alone Computers and Computers connected to the Networks may be referred and followed.

---

<sup>9</sup> **Competent Authority:** The Head of the Office or an officer expressly designated by the Head of the Office as the Competent Authority.

2.5 Random checks of telephone bills and PBX / EPBX call records may be carried out to ensure that no unauthorised INTERNET connections have been made from the Stand Alone/Network computers or by connecting Laptop or other electronic devices or by enabling the internal modem.

\*\*\*\*\*

CHAPTER -3

NETWORK COMPUTERS

**Installation Precautions**

3.1 Before the Network is installed, the Network Architecture should be got designed by a Certified Network Engineer and approved by the System Division.

3.2 Devices to be deployed in the Network including Servers, Terminals, Switches, Routers, Scanners, Back-up Devices, Cable Category, Racks, Storage Devices, storage methods and techniques should be listed properly and got approved by the Competent Authority. No deviation should be allowed without studying the implication of the deviations by a Certified Network Engineer.

3.3 The Security Policy of the Network should be documented before implementation of the Network. Access permission of each user should be clearly spelt out in the Security Policy.

3.4 Only Network specific Printers and Scanners should be used and it should be connected through the Network, and not directly to the client terminal.

3.5 No Terminal should have writing devices with the exclusion of internal hard disks. All such devices (Floppy Drive, CD/DVD Writer, Pen Drive, Scanner, etc) should be removed.

3.6 All unwanted Communication Ports (RS232, etc) and interfaces for Bluetooth and other such Wireless Devices should be blocked to prevent connectivity to unauthorised external sources.

3.7 All USB Ports should be blocked in the Client Terminals.

3.8 There should be no provision for remote connection to the Maintenance Company for sending alerts and carrying out maintenance through remote connection.

## **Network Administration**

3.9 Each Branch/Unit having LAN should designate a properly trained Network Administrator (NA)<sup>10</sup>, who would be responsible for operation/functioning of the Network and monitoring of the Security.

3.10 The NA should regularly undertake the review of the Network and take adequate measures to provide physical, logical and procedural safeguards for its security.

3.11 Since the NA shall have full control over the Network, an officer of high integrity should be appointed as the Network Administrator.

3.12 In case of a Server is being used for Classified Applications, it is advisable to have two NAs at a time and the passwords should have one part each from each NA should not disclose to the other under any circumstances.

## **Password**

3.13 Every individual user should have a separate user ID and Password. Two or more users should not share the same user ID and Password.

## **Access Control**

3.14 Access to the Server should be restricted.

3.15 The shareable data in a Network should reside in the Server. However, the non-shareable data may reside in the Client terminal with proper data security measures.

3.16 Biometric Access Systems (BAC systems) should be implemented in all the client terminals.

3.17 The Network should have Firewall<sup>11</sup> and Intrusion Detection Systems (IDS)<sup>12</sup> to detect/prevent unauthorised access.

3.18 Unwanted/unnecessary services like FTP, TELNET and Ports should be disabled.

---

<sup>10</sup> **Network Administrator:** The person responsible for maintenance and management of the computer network as well as assisting its users. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity; enforcing licensing agreements, developing a storage management program and providing for routine backups.

<sup>11</sup> **Firewall:** A protective Filter for messages and logons.

<sup>12</sup> **IDS:** IDS scans the Network for unauthorised Access/ Action.

## **INTRANET (WAN/MAN/LAN) -INTERNET**

3.19 INTERNET should not be connected to the branch/ unit Network under any circumstances.

3.20 The Network and INTERNET Terminals, Connection and Switches should be kept far apart to prevent any mix up/patching.

### **Disaster Recovery/Management**

3.21 System Division, each branch/ unit should develop a Disaster Recovery Plan (DRP), to ensure that in the event of failure of the Information System or destruction of the Facility, essential level of Services is maintained and Data restored. The DRP should include:

- Emergency procedures
- Call back procedures
- Restoration procedures

### **Miscellaneous**

3.22 Security of Racks housing the Switches, Routers, Hubs, etc. should be the personal responsibility of the Controlling Officer/ System Administrator<sup>13</sup>. Rack should always be locked and the key should remain in custody of the System Administrator.

\*\*\*\*\*

---

<sup>13</sup> **System Administrator** : A responsible official authorised by the competent authority for running, maintain and managing the computer system and its resources

## **CHAPTER -4**

### **INTERNET**

4.1 The Computer used for creating and storing official documents information should not be connected to INTERNET. This is as bad as keeping the doors wide open for the Intruders.

4.2 If an INTERNET connection is given to an official in his room, whether it is a dial up connection or broadband connection or Network connection of the INTERNET Room, it should be only on a separate computer, other than the computer used for office work. Care should be taken to keep the INTERNET computer and communication line socket far away from the office work computer.

4.3 All unwanted Services, Ports and Accessories should be disabled in the INTERNET computer.

4.4 It is advisable to provide INTERNET facilities in a designated INTERNET Room and providing individual INTERNET connection may be avoided

4.5 In case of broadband connection, the modem should be configured suitably to ensure security. The modem should be tested thoroughly to ensure that it does not permit any other remote connections.

4.6 Details of all visitors to the INTERNET Room should be available with the officer in charge with log in time, log out time, name of the officer and rank, etc.

4.7 Audit trail utility may be enabled in' Internet Computer to log all events.

4.8 No user should be allowed to bring in any kind of CSM for taking downloaded material or uploading any material from such a media.

4.9 If soft copy is required by an user, the request may be made to the officer in charge of the INTERNET Room, who may give the copy in a floppy or CD/DVD depending on the volume of downloaded material.

4.10 If print out is required, the same procedure as stated above may be followed.

4.11 Official Laptop computer should not be allowed to the INTERNET Room to connect to the network or for any other purpose.

4.12 No Classified office work should be done in any of the INTERNET linked computers.

### **E-Mail Communication**

4.13 E-mail for official communication should be in consonance with the Government Policy in vogue.

4.14 E-Mail account for official communications: should be opened with the authorised Govt. E-Mail service providers like NICNET, ERNET etc.

4.15 If an E-mail ID of NICNET / ERNET etc. has been obtained by an officer giving his/her personal particulars for official purposes, an intimation for deletion of his/her E-mail I D may be sent to NICNET / ERNET after his/her retirement or resignation as otherwise his/her E-mail ID may be misused.

4.16 Websites should be hosted only with the authorised Govt. Organisation Web Servers.

4.17 In the event of installation of a separate INTERNET LAN SERVER should have additional Security Measures by installation of Proxy Server<sup>14</sup>, Firewall, ID etc.

\*\*\*\*\*

---

<sup>14</sup> **Proxy Server:** A server that receives Web requests from clients, retrieves web pages, and forwards them to clients. Proxy Servers improve performance for groups of users by caching retrieved pages. It also provides security by shielding the IP Addresses of internal clients.

## CHAPTER-5

### SAFE CUSTODY/RECORD KEEPING/DISPOSAL OF HARDWARE

#### **Accounting**

5.1 All CSM should be serially numbered and labeled with a sticker/ logo of the department/Organisation to distinguish them from the CSM brought from outside. The CSM should be numbered and sticker/logo pasted immediately after procurement and before issue to a user. Consumables like printer ribbon, toner, cartridge etc. should also be numbered.

5.2 As a first step, all available CSM may be serially numbered and sticker/logo pasted after a stock taking is done.

5.3 Same guidelines may be followed for computers, printers, scanners, routers, switches, modems and other accessories also.

5.4 Each user unit should maintain a register for proper accounting of computers, accessories, external storage drives, Software items and CSM for proper accounting of the items available with the user.

5.5 The computer cell/store unit should supply blank Floppies/CDs/DVDs/ Cartridge Tapes etc., for use only against a written requisition duly signed/countersigned by an officer not below the rank of DySP or equivalent.

5.6 On receipt of blank Floppies/Cartridge Tapes/CDs/DVDs, Zip Disks, Pen Drives, SD Cards and other CSM, the user should take them on record in a register or appropriate software programme to be maintained for the purpose as per pro-forma below.

<i>Date</i>	<i>No. of floppies/ cartridges tapes/CD brought forward</i>	<i>No. of floppies/ cartridge tapes/CD received</i>	<i>Total No. of floppies/cartridge tapes/CD in stock</i>	<i>Sl. No. of floppies/cartridge tapes/CD</i>	<i>Date on which brought into use</i>
(1)	(2)	(3)	(4)	(5)	(6)

<i>Date on which floppies/cartridge incharge tapes/CD was rendered unserviceable (7)</i>	<i>Date and method of destruction (8)</i>	<i>Balance (9)</i>	<i>Remarks (10)</i>	<i>Sign. Of officer (11)</i>

5.7 Laptops/Pen Drives/External CD Writers/External DVD Writers/ Back up devices should be under the personal custody of the officer in charge of the store or the unit. These devices may be issued for use against written demands to an authorised officer for a specific work, which also may be recorded in the register maintained for issue of such items. As soon as the work is over the item should be taken into personal custody and necessary entries made in the register recording its return by the user officer.

5.8 Before issue of the item next time, the Controlling Officer may carry out a thorough check to ensure that no traces of the last work done in the device are still available in the device. If any traces of previous work are available steps may be taken to remove such traces before issue to the next officer.

### **Safe Custody**

5.9 Safe custody of every used Floppy/Cartridge Tape/CD/DVD/ SD Cards, Pen Drive etc., should be the personal responsibility of the officer concerned. .

### **Destruction/Weeding**

5.10 Damaged and unusable Floppies/Cartridge Tapes/CDs/DVDs/ Pen Drives and other CSM should be broken and destroyed by burning or as applicable to the weeding out of paper based files and an entry to this effect be made in the register.

5.11 Bad/condemned hard disk should not be released even after it has been replaced by a new one. Such hard disks may be destroyed by following procedures as applicable to weeding out of classified files.

5.12 Destruction should be carried out by application of corrosive chemicals (acids) or abrasive substance (emery wheel or disk sander) to the recording surface, and by shredding, incineration, disintegration, pulverisation and smelting etc.

**CHAPTER -6**

**CSO/ CISO & COMPUTER SECURITY AUDIT**

6.1 Senior System Analyst (SSA) has been designated as the Nodal Cyber Security Officer (**CSO**) and Chief Information Security Officer (**CISO**)<sup>15</sup> to coordinate and supervise all cyber security measures in Central Bureau of Investigation under control and supervision of Joint Director (Policy).

6.2 Periodic Security of the Computer and the Network should be carried out to ensure that the laid down guidelines are strictly followed.

6.3 Periodic Computer Security Awareness Programme (**CSAP**) for the computer operators, users and administrators should be carried out to expose them to the latest developments in cyber security and remind them of their responsibilities.

---

<sup>15</sup> Refer Policy Division Office Memorandum dated February 7, 2007

**CHAPTER -7**

**DO'S & DON'TS FOR COMPUTER OPERATOR/ USER:**

Some guidelines in the form of **Do'S and Don'ts** are enumerated below:

**DO'S :**

- 7.1 Restrict access to the authorized persons only.
- 7.2 Adopt effective access control procedures by incorporating proper identification and authentication mechanisms like 'Complex Passwords' at different levels, BAC System and 'Dynamic log-in' which verify the user's identity through magnetic strip cards, finger prints and voice recognition, depending upon the nature of sensitivity of the data.
- 7.3 Take necessary precautions against natural/ manmade hazards like fire, rain, dust, etc.
- 7.4 Use UPS units to prevent damage to Computer Hardware, Software and Data due to power fluctuation.
- 7.5 Use Hardware locks in the cabinets in which the computer system is housed.
- 7.6 If the computer system is used for very sensitive applications, use metallic shields cabinets in the room.
- 7.7 Boot level password should be enabled on the system.
- 7.8 Screen Saver Password should be used.
- 7.9 Software tools like Device lock may be used to block unwanted storage devices/ drives, ports and other external accessories.
- 7.10 Incorporate 'Audit Trail Concept' in the system as far as possible to know the date and time for which the users had used the system.
- 7.11 Take periodic backup of Software and Data on Floppies, CD's /DVDs or Cartridge Tapes and keep them under safe custody. One copy of the backup may be kept at a different location.
- 7.12 Take enough precautions against computer viruses by not allowing any outside Floppy or E-mail attachments for use without scanning for viruses. Have the latest virus signatures loaded on the DOS/ WINDOWS Operating System based computers.

- 7.13** Before deleting sensitive files, overwrite them several times (7 times and above) with some junk data to prevent restoration of the original data by any means.
- 7.14** Keep the Software Maintenance Tool (SMT) for detecting and rectifying any fault in the Software, in proper custody. Outside service engineers should be allowed to use their own Floppies as under this cover they may copy data from the system. The SMTs should be made available to the service engineers, as and when needed.
- 7.15** Copying, Deleting, Modification of Data or Printing any information from the system should be done under proper authorization.
- 7.16** All Floppies, Cartridge Tapes/ re-Writeable CDs/DVDs and other data recording devices issued to users should be sequentially numbered preferable with the organization's logo. Proper records of these media should be kept and periodical checks carried out.
- 7.17** Consider Floppies/ Cartridge Tapes and Re-writeable CDs/DVDs, Pen Drives, SD Cards etc. as sensitive documents. Exchange of Floppies, Cartridge tapes and Re-Writeable CDs/DVDs etc. should be dealt with the same security procedures as required for hard- copies of documents.
- 7.18** Damaged and unusable floppies/ Cartridge Tapes and Re-writeable CDs/DVDs, Pen Drives, SD Cards etc should be broken into pieces and destroyed by burning and a record of such destruction should be maintained.
- 7.19** All used printer ribbons, carbons, draft memos and reports, unused printouts, etc. should be destroyed by burning.
- 7.20** Rectification of faults and maintenance should be carried out under proper and close supervision.
- 7.21** In case the shift system is in vogue, there should be proper handing & taking over of charge between shifts in charges.
- 7.22** Use effective encryption techniques while communicating sensitive information over the communication network. Commercially available encryption devices are not safe as their algorithm and decryption keys are known to others.
- 7.23** Carry out periodical verification of character and antecedents of computer personnel handling critical functions.
- 7.24** Use effective identification, authentication and acknowledgement while exchanging information between two remote locations.
- 7.25.** Use exclusive computer for INTERNET. No office work whatsoever should be done on this computer.
- 7.26.** Keep skills and knowledge current.

**Don'ts :**

- 7.27.** Don't let any unauthorized person use your computer system.
- 7.28.** Don't share your 'Password' with anyone, not even your colleagues.
- 7.29.** Don't reveal the 'root password' to any unauthorised person.
- 7.30.** Don't connect the computer directly to the mains.
- 7.31.** No heavy electric load drawing machines like plain paper copier, shredding machines, coolers, etc. should be connected to the source of constant voltage power supply to the computer.
- 7.32.** Don't connect your computer system storing classified data to INTERNET.
- 7.33.** Don't allow staff members to bring their own Floppies/ Re-Writeable CDs/DVDs, Pen Drives, SD Cards etc. to run on the computer system of the department.
- 7.34.** Don't Use pirated or gifted copies of Software as these may contain Virus and even facilitate intrusion into the system.
- 7.35.** Don't load games in your computer. These could be the main carriers of computer Viruses and an unsuspecting easy medium for an intruder to break into your computer system.
- 7.36** Don't loan Software Program Disks/ Re-Writeable CDs/DVDs, Pen drives, SD Cards etc., as these may be returned with Virus. If however, it becomes unavoidable, loan only a copy and not the original media.
- 7.37** Do not use internal CD/DVD Writer or COMBO drives, unless specifically authorized.
- 7.38** Do not use any Pen/ Flash drive/ SD Cards, unless specifically authorised.
- 7.39** Don't connect communication (TP or PC-PC) computer to your LAN.
- 7.40** Don't boot the system from the advance point. Follow systematic booting procedures.

**Confidential**

**Central Bureau of Investigation  
Policy & Coordination Division  
North Block, New Delhi**

**February 28, 2007**

**Circular No.6/2007**

**Subject: Computer Security Guidelines – Version 1.**

A copy of a booklet titled “Computer Security Guidelines” Version 1, is enclosed for guidance of SsP/ DIsG. The contents may be shared with all the officers using computers in the branches/ units.

The receipt of the booklet may be acknowledged.

This issues with the approval of Director, CBI.

Sd/-  
**( Navneet Rajan Wasan )**  
**Joint Director (Policy)**

Encls: [As above.](#)

Copy to:

1. All DIsG (By Name)
2. All SsP/ SSA (By Name)
3. All ALA's
4. All Joint Directors, DoP
5. SDCBI(S) & ADCBI(A)
6. PS to DCBI
7. Guard File.

File No.21/8/2007-PD/506