GOVERNMENT OF INDIA
DEPARTMENT OF PUBLICATION
CIVIL LINES, DELHI – 110 054.
Website: www.deptpub.nic.in
Email: acop-dep@nic.in (&) pub.dep@nic.in
TEL.: 2381 7823 / 2381 9689 Fax: 2381 7846.

No.19/O&M/2014 Dated: 30th June, 2014

CIRCULAR

Subject: Information Security Instructions Booklet for Ministry of Urban Development.

A copy of Ministry of Urban Development's Office Memorandum No. I-11011/40/2009-Admn.III. dated 09.4.2014 is enclosed herewith.

All Branch Officers/Section In charges of this Department are directed to follows the instruction mentioned at Point 4 of the Information Security Booklet for Ministry of Urban Development.

(A.K. Singh)
Asstt. Controller (Business.)

Copy to:

1. P.A. to J.S. & C.P.
2. P.A. to A.C.(A)
3. P.A. to F.O.
4. P.A. to A.C. (B)
5. All Section In charges
6. S.O. Kitab Mahal, estate Emporium Building, Baba Kharg Singh Marg, New Delhi
7. Sale Counter, Delhi High Court, New Delhi
8. Hindi section for Hindi version.
9. E-Gazette Section for uploading on this Department's website.
10. Notice Board.
11. Guard File

4. General Instruction for Acceptable Use of IT Resources

- All PCs, laptops & workstations should be secured with a password protected screensaver with automatic activation feature set at 10 minutes or less, or by logging off when the machine is unattended. Passwords should be changed frequently.

- All hosts used by the official that are connected to Internet/ Intranet shall be continually executing virus scanning software and with uptodate operating system patches

- Users shall not copy or install any software on their own, including privately owned shareware, freeware or through CDs/DVDs without prior approval of competent authority.

- Information contained on portable devices such as tablets, smart phones & laptops is especially vulnerable. The officials should not leave their mobile devices unattended in public locations (eg. Meeting-rooms, airport lounges, restaurants etc..) It is advised that Laptops/USBs of Higher Officials should have encryption technologies & Biometric authentication to prevent information misuse in case of theft.

- Use of external storage devices by default will not be allowed to the Government framework, except with due approval from competent authority.

- Employees must use extreme caution while opening email attachments received from unknown senders which may contain viruses. Officials must not access private email servers from Govt. of India network nor use their services for any official correspondence.

- The users are responsible for maintaining the security of the Internet application services including protection of account details & passwords, thereby protection of unauthorized use of their application services by a third party.

- Personal Information shared on social media network can be used to design a particular attack against a particular department. Hence an officer may not identify himself as a public servant. He shall not click on any link shared during an IRC in chats and discussion forums as it can lead to downloading of malicious code on a Govt. network accessible device.

- Users should be careful when trying to access Govt. network from public kiosk or insecure networks for eg. Email services. They should use VPN/OTP to connect to Govt. IT resources.

- Users shall be deterred from using information processing facilities for unauthorized purposes.

- Media may be disposed of securely and safely when no longer required, using formal procedures. This include Hard disks, CDs/DVDs & pen Drives etc..

- Formal exchange policies, procedures and controls shall be in place to protect the exchange of information through the use of all types of communication media.

- Inventory of all hardware & networking IT assets of the organization should be clearly identified & maintained along with Ownership information labeled on the asset & also maintained centrally with the administration for all the information processing facilities accessed by the client, In case of breach of security for fast isolation, containment of the breach & recovery from the disaster.