Best Practices for Use of IT Devices

On

Government Network

April 2014
Version 1.0

Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
New Delhi - 110003

Contents

1. Introduction:

Government of India has formulated the **"Policy on Use of IT Resources"**. This document supports the implementation of this policy by providing the best practices related to use of desktop devices, portable devices , external storage media and peripheral devices such as printers and scanners.

2. Desktop Devices

2.1 Use and Ownership

Desktops shall normally be used only for transacting government work. Users[1] shall exercise their own good judgement and discretion towards use of desktop devices for personal use to the minimum extent possible.

2.2 Security and Proprietary Information

a. User shall take prior approval from the competent authority [2] of their respective organizations [3] to connect any access device to the Government network.

b. User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy available at http://www.deity.gov.in/content/policiesguidelines under the caption "Policy of Use of IT Resources".

c. All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.

d. Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

e. User shall report any loss of data or accessories to the competent authority of their respective organization.

f. User shall obtain authorization from the competent authority before taking any Government issued desktop outside the premises of their organization.

g. Users shall properly shut down the systems before leaving the office.

h. In case an organization does not have two networks, as recommended in the Policy on "Use of IT Resources" Classified/ sensitive data shall not be stored on the desktop connected to the internet.

i. Users shall encrypt all sensitive information while storing it on the desktop.

j. By default all interfaces on the client system shall be disabled and those interfaces that are required are enabled.

k. Booting from removable media shall be disabled

l. Users shall be given an account with limited privileges on the client systems. User shall not be given administrator privileges.

m. Users shall abide by instructions or procedures as directed by the IA [4] /Nodal agency [5] from time to time.

n. If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the IA/Nodal Agency for corrective action.

2.3 Use of software on Desktop systems

a. Users shall not copy or install any software on their own on their desktop systems, including privately owned

shareware and freeware without the approval of the competent authority.

b. A list of allowed softwares shall be made available by the IA. Apart from the Software's mentioned in the list, no other software's will be installed on the client systems. Any addition to the list by the respective organizations should be done under intimation to IA.

2.4 Sharing of data

Users shall not share their account(s), passwords, security tokens (i.e. smartcard), Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

2.5 Use of network printers and scanners

a. User shall use a strong administrator password on the device to help defend against attacks and to prevent re-configuration by an unauthorized user.

b. Where the device supports Access Control Lists (ACLs), the devices shall be configured to block all traffic from outside the Organization's IP range.

c. FTP and telnet server on the printer shall be disabled.

d. User shall disable any protocol or service not required.

3. Use of Portable devices

Devices covered under this section include Government issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices shall be governed by the following:

a. User shall be held responsible for any unauthorised usage of their Government issued access device by a third party

b. Users shall keep the Government issued devices with them at all times or store them in a secured location when not in use. User should not leave the devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).

c. User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy available in "Password Policy" at http://www.deity.gov.in/content/policiesguidelines under the caption "Policy of Use of IT Resources".

d. User shall ensure that remote wipe feature is enabled on the Government issued device, wherever technically feasible. Users shall not circumvent security features on their devices.

e. User shall ensure that the device has latest operating system, anti-virus and application patches. Firewalls shall be enabled, if possible.

f. Users shall wipe or securely delete data from the device before returning/ disposing it of.

g. Lost, stolen, or misplaced devices shall be immediately reported to the IA/Nodal agency and the competent authority of the organization.

h. Data transmissions from devices to the services on the Government network shall be over an encrypted channel.

i. When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

4.0 External Storage Media:

Devices covered under this section include Government issued CD/DVD's, USB storage devices etc. Use of these devices shall be governed by the following:

a. Use of external storage [6] media, by default shall not be allowed in the Government network. If the use of external storage is necessary, due approval from the competent authority of that respective organization shall be taken.

b. Blocking access to external storage on a Government issued access devices like desktop/laptop etc shall be implemented at all organizations within the Government. Users authorised by the competent authority of the organization to use the external storage will be allowed as per the policies configured by the IA/Nodal agency.

c. Users shall use only the media issued by the organization. The user shall be responsible for the safe custody of devices and contents stored in the devices which are in their possession.

d. Classified data shall be encrypted before transferring to the designated USB device. The decrypting key shall not exist on the same device where encryption data exists.

e. Classified/ sensitive information shall be stored on separate portable media. User shall exercise extreme caution while handling such media.

f. Unused data on USB devices shall be cleaned through multiple pass process (like wipe/eraser software)

g. Users shall not allow USB device belonging to outsiders to be mounted on Government systems.

4.1 Use of External storage media by a visitor

a. Competent authority shall ensure that process is in place that visitors to an organization shall not be allowed to carry any portable media without permission.

b. If it is necessary to allow the visitor to use a USB memory device for any reason, it shall be used only on designated systems meant for presentation purpose. Under no circumstances the USB device belonging to visitors shall be mounted on systems that are connected and belong to the Government network.

4.2 Authority issuing External storage devices of each organization shall adhere to the following:

a. Competent Authority of an organization shall ensure that process is in place to maintain records for procurement, issue, return, movement and destruction of the storage devices

b. All obsolete USB devices shall be physically destroyed to avoid misuse.

c. Self-certification for verification of USB devices by individuals at regular intervals of 6 months shall be carried out by issuing authority to ensure that devices issued to them are under their safe custody.

GLOSSARY

S.no	Term	Definition
1	**Users**	Refers to Government/State/UT employees who are accessing the Government services.
2	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his organisation
3	**Organisation**	Ministry/Department/Statutory Body/Autonomous body under Central and State Government
4	**Implementing Agency (IA)**	A Body which will be responsible for ensuring compliance with this policy with reference to network services including power to take precautionary and penal actions as specified in this policy.
5	**Nodal agency**	Respective organization responsible for ensuring compliance with this policy with respect to use of It resources except network services.
6	**External Storage**	In computing, external storage comprises devices that temporarily store information for transporting from computer to computer. Such devices are not permanently fixed inside a computer.