

Government of Gujarat
Department of Science & Technology
Circular No.: SWN/13/2010/4208/IT
Sachivalaya, Gandhinagar

Date: 10 DEC 2014

READ:

1. Government Resolution No.: SWN/132008/303097/DST, Dated 5th November 2009

INTRODUCTION:

Government of Gujarat has provided IT Devices such as desktops, portable devices, external storage media and peripherals like printers, scanners, etc. to a large number of State, District, Taluka and Village level offices across the State.

The objective of these policy guidelines is to follow the best practices on usage of such IT devices.

CIRCULAR:

Following policy guidelines shall be considered for the usage of IT Devices provided by Government of Gujarat:

1. Desktop/Laptop Devices

1.1 Use and Ownership

Desktops/laptops shall be used only for transacting Government work. Users shall exercise their own judgement and discretion to keep the personal use of desktop devices to the minimum extent possible. No one shall access any entertainment, social media or any business related websites using the internet provided by the Government or by using personal data card.

1.2 Security and Proprietary Information

- a. Users shall keep their passwords secure and shall not share their account details. Users shall keep strong and secure passwords as per the password policy available at http://gswan.gov.in/PDF/GSDC_Polices/Password_Policy.pdf under the caption "Password Policy".
- b. Users shall not give their computer or network facility passwords to any unauthorized person nor shall they obtain somebody else's password by any unauthorized means whatsoever. No one except the

system administrator in charge of a computer is authorized to issue passwords for that computer.

- c. Users shall not use the facility provided by the Government for purposes like playing games, listening to music, watching videos, etc. or for any other personal use.
- d. Users shall log-off when the system is unattended and all active desktop/laptop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less.
- e. Users shall ensure that updated virus-scanning software is installed & running in all systems. Users shall exercise due caution while opening e-mail attachments received from unknown senders as they may contain viruses or other malicious software.
- f. Users shall report any loss of data or accessories to the competent authority of their respective organization.
- g. Users shall not use the communication facilities of the device to interfere with others' legitimate use, of any computer or network facility anywhere.
- h. Users shall obtain authorization from the competent authority before taking any Government issued desktop/laptop outside the premises of their organization and to connect any outside computer to the Government networks.
- i. Users shall properly shut down their systems and turn off the power before leaving the office.
- j. 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 Head of the Department/Organization for corrective action.

1.3 Use of software on Desktop/Laptop systems

- a. Users shall not copy or install any software on their own on their desktop/laptop systems, including privately owned shareware and freeware without the approval of the Head of the Department/Organization.
- b. Users shall not share their account(s), passwords, security tokens (i.e. smartcards), Personal Identification Numbers (PIN), digital signature certificates or similar information, devices which are used for identification and authorization purposes, etc. with any unauthorized persons.

- c. Users shall take full responsibility for data that they store in their computers and transmit through network facilities.
- d. Users shall not use computers or network facilities to store or transmit data in ways that are prohibited by law or policy issued by State Government from time to time.
- e. User shall not transfer, install, or use any software or data files in violation of applicable copyrights or license agreements, including but not limited to downloading and/or distribution of music, movies, or any other electronic media.

1.4 Use of network printers and scanners

- a. A strong administrator password shall be used 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. Any protocol or service which are not required shall be disabled.

2. Use of Portable devices

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

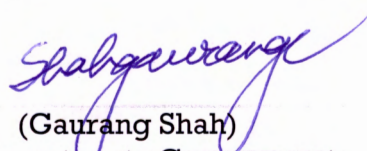
- a. User shall be held responsible for any unauthorized usage of their Government issued access device by a third party.
- b. Users shall keep the Government issued devices with them at all times or store them in a secured location when not in use. User should not leave the devices unattended in public 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.
- d. Users shall wipe or securely delete data from the device before returning/ disposing it off.
- e. Lost, stolen, or misplaced devices shall be immediately reported to the Head of the Department/Organization.

3. 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 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 authorized by the competent authority of the organization to use the external storage will be allowed as per the policies configured by the Head of the Department/Organization.
- 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. Extreme caution shall be exercise while handling such media.
- f. Unused data on USB devices shall be cleaned through multiple pass process.
- g. USB device belonging to outsiders shall not be mounted on the Government systems.
- h. 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.

By order and in the name of the Governor of Gujarat.



(Gaurang Shah)

Joint Secretary to Government,
Department of Science & Technology

To,

- Secretary to the Hon'ble Governor of Gujarat, Raj Bhavan, Gandhinagar.
- Chief Principal Secretary to Hon'ble C.M.
- Principal Secretary to Hon'ble C.M.
- Secretary to Hon'ble C.M.

- PS to Hon'ble Minister, Science & Technology.
- Deputy Secretary to the Chief Secretary, Government of Gujarat
- All Secretaries Department.
- The Chairman & Managing Director, Gujarat Informatics Ltd., Gandhinagar.
- The Secretary, Gujarat Vigilance Commission, Gandhinagar.
- The Secretary, Gujarat Public Service Commission, Ahmedabad.
- The Secretary, Gujarat Legislature Secretariat, Gandhinagar.
- The Registrar, Gujarat High Court, Ahmedabad.
- The Secretary, Gujarat Civil Services Tribunal, Gandhinagar.
- All Heads of Department.
- All Heads of Office.
- All Collectors.
- All D.D.Os.
- The Accountant General, (A&E), Gujarat, Post Box No.220, Rajkot.
- The Accountant General (A&E), Gujarat, Ahmedabad branch, Ahmedabad.
- The Accountant General (Audit)-1, Gujarat, M.S.Building, Ahmedabad.
- The Director of Accounts & Treasuries, Gandhinagar.
- All Treasury Officer.
- All Pay & Accounts Officers, Ahmedabad/Gandhinagar.
- Resident Audit Officer, Ahmedabad/Gandhinagar.
- Select file, S & T Department.