

GOVERNMENT OF PAKISTAN  
CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB)

\*\*\*


No. 3-4/2002 (NTISB-II)/ MS

Islamabad 21 November 2012

Subject:- USB/ Flash Drives/ Mass Storage Devices and its Security Parameters

The use of computers has increased manifold for speedy exchange of information in govt departments. A large amount of official/ sensitive data of almost every organization is residing in its IT systems/ PCs. Besides, other means, USBs/ flash drives are being used at large for storing/ carrying data from one place to the other. Though smaller in size, these drives have remarkable benefits and advantages such as high performance, durability and affordability etc, however there are a number of risks also associated with these drives such as sudden loss and spread of viruses etc. If not handled carefully, these devices can prove harmful to the resident data in computers/ IT systems and can also cause irreparable damage to the national/ organizational security. Extensive use of USBs/ flash drives and associated security risks warrant every govt organization to take appropriate measures and make their officials aware of these disadvantages/ security hazards to thwart any-unwanted incident.

Guidelines emphasizing benefits/ security hazards related to USBs/ flash drives as well as recommendations for its safe use are attached herewith (Annex A). All Ministries/Divisions/ govt departments are requested to disseminate this information to all affiliated/subordinate offices to create reasonable awareness and taking appropriate measures for safeguarding their official data, please

  
Lt Col  
(Malik Nadeem Akhtar)  
Deputy Secretary (NTISB)

All PS to Secretaries of Ministries/ Divisions (Federal Government) and Secretaries S&GAD (Provincial Governments) (list attached)

23 NOV 2012

M(A)

7 NOV 2012

C(A)

29/11

S(Exp)

SS(coord)

Disseminate

29/11

AW

Q

150517-R

150517-R

150517-R

150517-R

150517-R

## Guidelines

### Handling of USB/Flash Drives/Mass Storage Devices

Fast track development in the field of information and communication technology in the near past has brought a great revolution in the field of micro IT equipment manufacturing. Today, with ever increase Memory Storage Base, larger pieces of IT Memory/ Storage Devices gadgets have been transformed into more portable, convenient and durable shapes/ sizes with high performance. Like other IT equipment, these mass storage devices (MSD) have also been completely revolutionized and reshaped by increased data storage capability, smart circuit minimization with smart chip technology, high portability and compatibility with all operating systems. Though smaller in size, these drives are associated with remarkable benefits and advantages such as high performance, durability, sustainability, reliability and affordability.

2. Despite a plenty of benefits and advantages, these storage drives/ devices are associated with a number of disadvantages and at times pose high security risks. If not handled carefully, these devices can not only prove harmful to the resident data in computers/ IT systems but can also cause irreparable damage to the organizational/ departmental security/ integrity. In case of govt organization, any breach/ loss of data may have profound impacts on day to day govt business and hence warrants due consideration. Some of the vital security concerns and risks associated to the USB drives are as under:-

- a. The most obvious security risk for USB memory devices is of their sudden loss, misplacement or being stolen due to their small size. If the data was not backed up properly, the loss of a USB drive can mean hours of lost work and with the potential threat of replicating data/ information to some unwanted/ undesirable source. If not encrypted properly, the whole data can be recovered/ accessed. Though seemingly a very common memory device, but can have serious consequences if handled carelessly.
- b. Any persons with malicious intentions may also use their own USB drives to steal any vital information directly from a computer source. If

an attacker has been able to gain physical access to a computer/ network of any organization, he can easily access/ download sensitive data/ information directly onto a USB drive.

- c. Computers/ Machines in the process of being turned off. may be vulnerable, because a computer's memory is still active for some time. Just by plugging a USB drive into the computer, the attacker can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data in the drive. Victims may not even realize that their file systems have been compromised and if so, it may be too late to react.
- d. It has been observed in some infected USB drives that the command "DELETE" is taken as the command "HIDE", this is what we call the FAT (File Allocation Table) recovery issue. Apparently a file is "deleted" from USB flash drive or a "Quick Format" is performed to "delete" all files and it seems as if all such files/ data no more exists and is "Deleted". But in fact it only hides the data from your view instead of deleting or formatting, thus this phenomena could cause misconception or can be catastrophe depending on the amount of data stored.
- e. USB/ Flash drives are the prime source for spreading various types of viruses/ worms/ malwares. A computer might be infected with malicious code or malware that can detect/ infect a USB drive automatically on being plugged into a computer. Similarly, when this virus-infected USB drive is plugged into another computer, the host computer also gets infected by virus/ malware infected USB. In such a way, infected USB drive becomes a permanent source for spread of virus/ malware initiating chain of infections to number of computers.
- f. These days Bluetooth technology enabled devises including mobile phones, USB sticks, laptops and other IT microtech related devices are very common with fast and easy data transfer capability from one

source to the other. Acquisition of such data from Bluetooth enabled USB to any other USB source may result huge transfer of data on wireless, giving an edge to the suspect on the one hand and a source of sheer loss of vital information.

3. Keeping in view some of the key vulnerabilities of USBs as mentioned above and in view of the sensitivity of the subject, it is suggested that strict implementation policy must be devised to protect government sensitive data by formulating simple SOPs under respective Ministries/ Divisions/ Govt departments to ensure foolproof security of stored/ backup of vital data by adopting following measures:-

- a. Ensure that only patent proprietary licensed antivirus/ malware software programme is installed on the server domains/ PCs and updating them regularly.
- b. Buy only genuine USBs flash drives from recognized source/ company, contained in genuine, air tight, non-tampered/ sealed manufacturer packaging, hermetically sealed plastic envelope and avoid purchasing cheap quality devices.
- c. Keeping the "Autorun" option unchecked from the dialog box appearing on connecting the USB to computer, thus avoiding any direct threat.
- d. Do not leave the PCs/Laptops unattended with improper shutdown/ switching off, this may result into any possibility of hacking.
- e. Establish proper and safe mechanism for taking USBs/ official equipment (CPUs and USB drives etc) out of the govt premises/ offices for any repair/ other purposes.
- f. Strictly follow the purchase/ repair policy of IT equipment (USB drives and PCs) by authorized vendors only. A mechanism for purchase/repair of IT equipment should be prepared and a list of authorized vendors should be published for this purpose.
- g. Always maintain a backup file in your office hard disk in case of loss of data from USB, followed by prompt reporting to higher authorities.

- Action by Computer*
- Return by*

**h.** Disable the Bluetooth option in all Bluetooth enabled USBs/ Flash drives while any work is in progress. Sharing of files should be restricted through LAN only.
  - i.** USBs considered useless, faulty or defective must be disposed off correctly through proper channel by destroying it completely to avoid any possible data recovery.
  - Return by*

**j.** USB ports may be disabled in all wings/sections of official computers. Ports will be made enable only in administrator login. USB ports and DVD drives should only be enabled on the official computers deemed necessary.
  - Computer*

**k.** Use of personal USB may be strictly prohibited.
  - l.** Only official USB may be used with the approval of competent authority.
  - m.** Official USB may be kept with network administrator or kept with the concerned officer of the section and to be issued with written permission.
  - n.** Official USB may be used only for official purpose and not be allowed to carry it outside.
  - Return by*

**o.** Latest antivirus may be installed on all office computers particularly with network administrator who will perform scanning before and after issue of USB.
  - Return by*

**p.** If possible, a software may be installed on all computers which keep the log of all USBs attached/detached with that computer.
  - Return by*

**q.** If feasible , AES (Advance Encryption Standard) USB flash drive may be used for protection and safeguarding the sensitive and classified information.

\*\*\*\*\*