"Autorun virus" Removal Procedure
Version 1.1

What is "Autorun virus" ?

"Autorun virus" is a popular computer virus recently. The virus exploits the mobility of external storage device and the autorun feature of windows operating system to spread. It creates an executable file on the infected computer and an autorun.inf file on all writeable disk drive, it also disables the display of hidden files. If an infected computer can mount any writable network disk drive or external storage media (eg. USB Flash drive, USB hard disk, various memory card and MP3 player etc), virus file will copy itself to these devices automatically.

IMPRORTANT NOTES

- This procedure is used for removing Autorun virus. You should follow **ALL THE STEPS IN ORDER**.

- Before modifying the system, you should **backup you data** so that you can restore your system to the original state if there is any problem (eg. copy document files, photos, address book, etc. to CD-R/DVD-R.)

- All data and information provided in this procedure are for informational purpose only. The users should take full responsibility in deciding whether to follow the steps in the procedure and to remove the "Autorun virus" from their machines. HKCERT will not liable for any errors or omissions in the content of this procedure, nor for any damages or losses arising from any actions taken in reliance on the information provided.

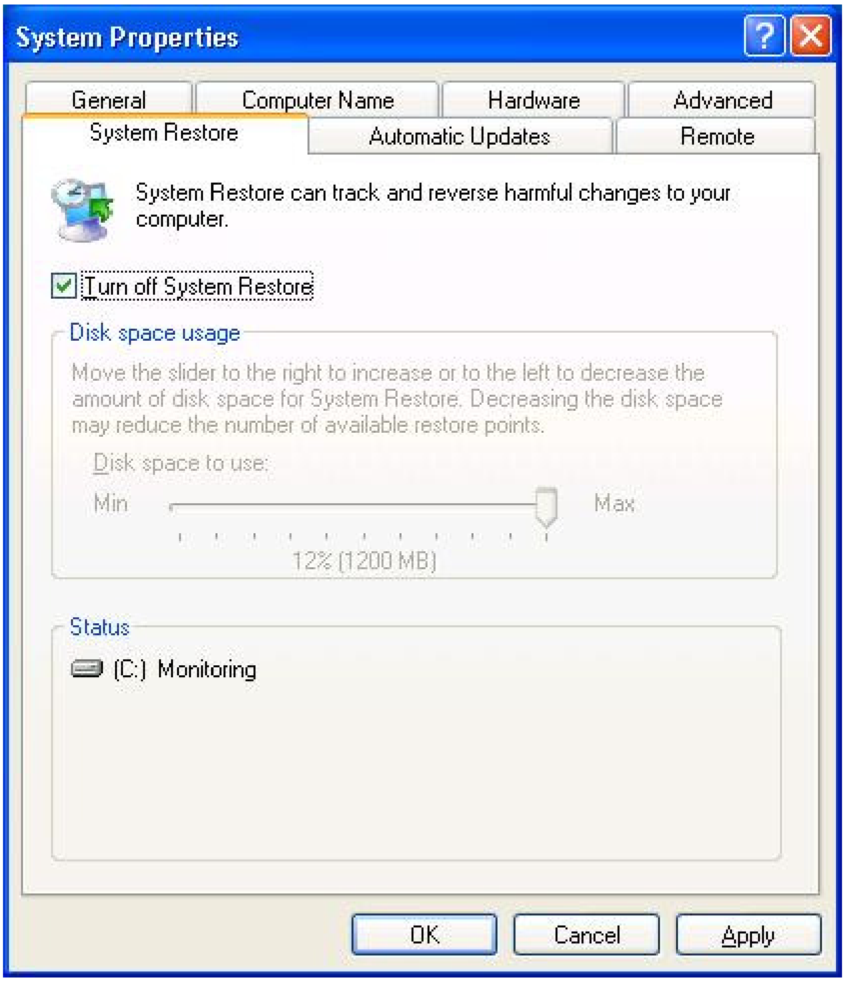
- It you have any query on this procedure, please contact HKCERT.
Tel: 81056060; Email: hkcer@hkcert.org

Since "Autorun virus" does not have a reliable removal tool, a "manual removal" is required to fix it. This procedure applies to Windows 2000, Windows XP, Windows 2003 and Windows Vista, please follows all the steps in order:

1. Disconnect the infected computer from the network (If the infected computer more than one, please fix the server in a higher priority), eg. Disconnect the network cable. Otherwise the virus can spreads to other computers on the same network.

2. Close the system restore function (Only apply to Windows XP and Windows Vista) Why do we have to disable the system restore ? – Windows system restore function creates and saves the "restore points" regularly (Default is daily) or certain changes detected, eg. Install software and driver also creates a new "restore point". "Restore points" includes Windows registry keys and other system data but not include personal files (such as Email, Document and Photo). To avoid the system to keep the virus files and associated registry keys on the "restore points" and may waste our effort. We have to close the system restore function to clear the content in the "restore points".

i. For Windows XP
Click "Start".
Right-click "My Computer", and then click "Properties".
Click the "System Restore" tab [See Figure 1].



System Restore can track and reverse harmful changes to your computer.

☑ Turn off System Restore

Disk space usage

Move the slider to the right to increase or to the left to decrease the amount of disk space for System Restore. Decreasing the disk space may reduce the number of available restore points.

Disk space to use:

Min Max

12% (1200 MB)

Status

(C:) Monitoring

[Figure 1]

Check the "Turn off System Restore" or "Turn off System Restore on all drives", and then click “Apply”.

As show on the message windows, all existing restore points on your computer will be deleted, click “Yes”

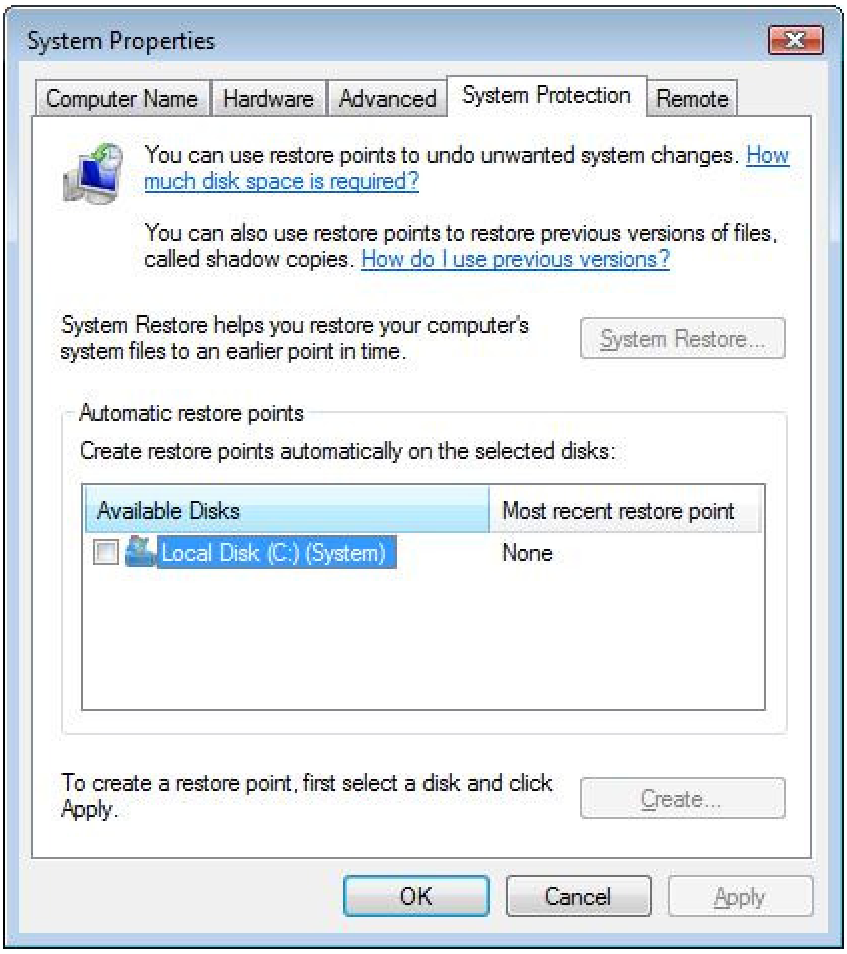
Click “OK”, restart the computer.

ii. For Windows Vista

Click Start.

Right-click “My Computer”, and then click “Properties”.

Click the “System Protection” tab [See Figure 2].



You can use restore points to undo unwanted system changes. How much disk space is required?

You can also use restore points to restore previous versions of files, called shadow copies. How do I use previous versions?

System Restore helps you restore your computer's system files to an earlier point in time.

Automatic restore points

Create restore points automatically on the selected disks:

Available Disks	Most recent restore point
□ Local Disk (C:) (System)	None

To create a restore point, first select a disk and click Apply.

[Figure 2]

On “Available Disks”, uncheck the Local Disk (Default is C).

As show on the message windows, all existing restore points on your computer will be deleted，click “Turn System Restore Off”

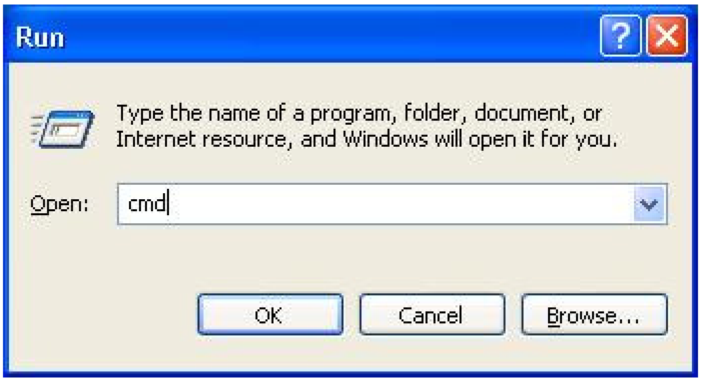
Click “Apply” and then click “OK” to confirm.

Restart the computer.

3. Remove the virus files

i. Open windows explorer, records the existing drive letter.

ii. At “Start”->”Run”, input cmd [See Figure 3] and click “OK”, a command prompt occurs.



Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

cmd

[Figure3]

iii. Check the existence of autorun.inf file

Input cd \ ，back to C:\

Input attrib autorun.inf

If you find autorun.inf file, input type autorun.inf

You can see the file content as below:

```
open=[xxx]
shell\open\Command=[xxx]
shell\explore\Command=[xxx]
```

Note: [xxx] stands for the virus file name, the file name on each infected computer may be varied, please records [xxx] file name.

iv. del autorun.inf and virus file

Input attrib -S -H -R X:\autorun.inf

Input attrib -S -H -R X:\[xxx], if this file was deleted or not exist, a file not found error message will be showed.

Note: [X] stands for the drive letter, all the storage media attached to the computer. (includes Network, USB storage device and different memory card), [xxx] stands for the virus file name

Input del X:\autorun.inf

Input del X:\[xxx]，if this file was deleted or not exist, a file not found error message will be showed.

Note: Please input the file being deleted carefully. Otherwise, it may delete the normal files.

Execute the above steps on each drive. After finished, type “exit” to quit the command prompt window.

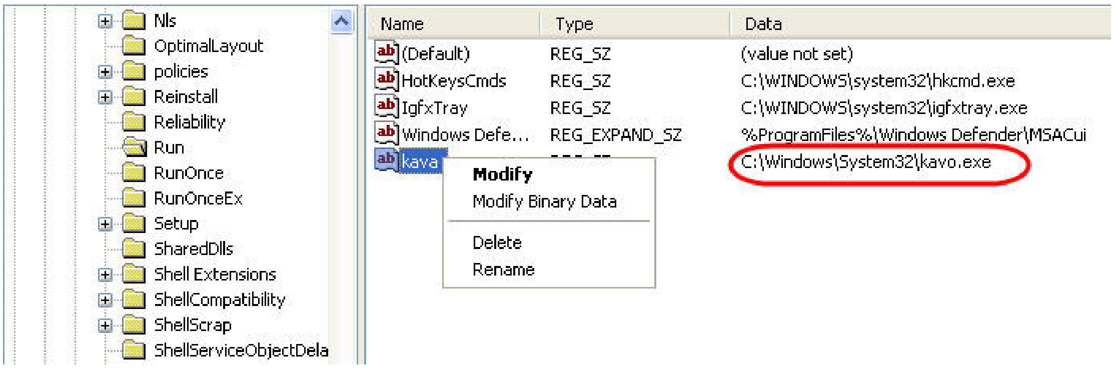
4. Delete the registry key of the virus for execution.

> Note: The below procedure requires using “Registry Editor” to restore the windows registry keys, if you are not familiar with windows registry operation, please ask your computer vendors or friends for assistance. Improper change on windows registry key may cause the windows malfunction.

At “Start”->”Run”, input regedit and click “OK”, a registry editor window occurs.
At HKCEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
and
At HKCEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Search the following registry key value [See Figure 4]
i. Windows 2000 registry keys
C:\WINNT\System32\[yyy]

ii. Windows 2000 registry keys and Windows 2003 registry keys
C:\WINDOWS\System32\[yyy]



Name	Type	Data
(Default)	REG_SZ	(value not set)
HotKeysCmds	REG_SZ	C:\WINDOWS\system32\hkcmd.exe
IgfxTray	REG_SZ	C:\WINDOWS\system32\igfxtray.exe
Windows Defe...	REG_EXPAND_SZ	%ProgramFiles%\Windows Defender\MSACui
kava	[illegible]	C:\Windows\System32\kavo.exe

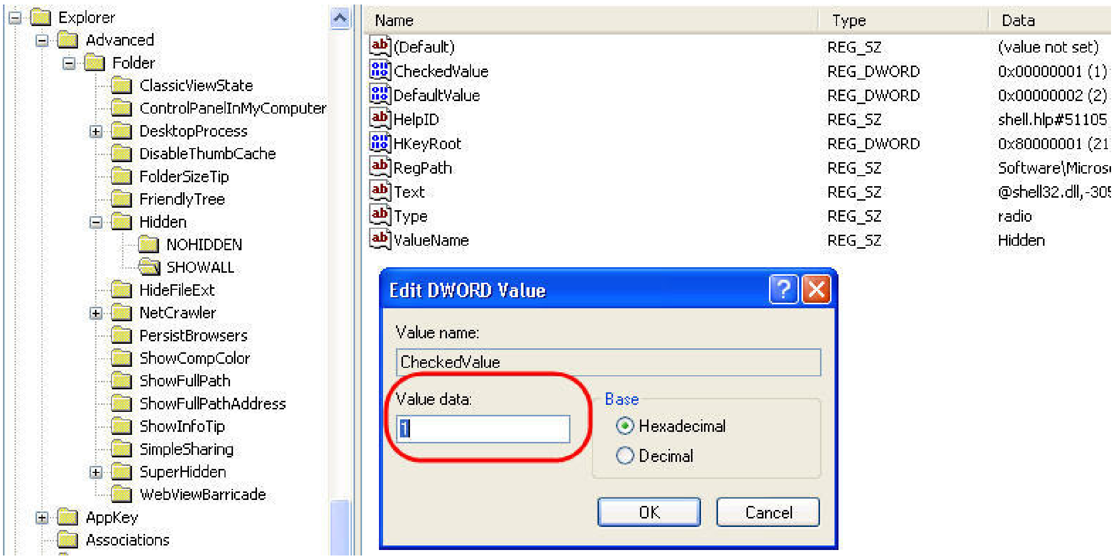
[Figure 4]

Note: [yyy] stands for virus file name, eg. fly.exe, goods.exe, kavo.exe, kavo0~9.dll, mnso.exe, ntdelect.com, ntdelete.com, nx.exe, poor.exe, rxpmon.exe, sos.exe, systom.exe, taso.exe, taso0~9.dll, tavo.exe, ubs.exe, winpows.exe (list is not exhaustive) etc., the file name on each infected computer may be varied. If found, please records file name [yyy] and delete this registry key. If nothing found, please follows the step 7 to use your antivirus software or online virus scanning tools to run a full system scan and deletes the infected files.

5. Resolve the display of hidden files problem

At HKCEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL [See Figure 5]

Search CheckedValue registry key, open it and change the value to 1.



Name	Type	Data
(Default)	REG_SZ	(value not set)
CheckedValue	REG_DWORD	0x00000001 (1)
DefaultValue	REG_DWORD	0x00000002 (2)
HelpID	REG_SZ	shell.hlp#51105
HKeyRoot	REG_DWORD	0x80000001 (21
RegPath	REG_SZ	Software\Micros
Text	REG_SZ	@shell32.dll,-30
Type	REG_SZ	radio
ValueName	REG_SZ	Hidden

Edit DWORD Value

Value name: CheckedValue

Value data: 1

Base

● Hexadecimal

○ Decimal

[Figure 5]

6. If the steps (3-5) cannot delete the virus files, please reboot the computer and press F8 consecutively，select to use “Safe mode” to boot into windows. Open windows explorer, delete the previous logged [xxx] and [yyy] virus files manually.

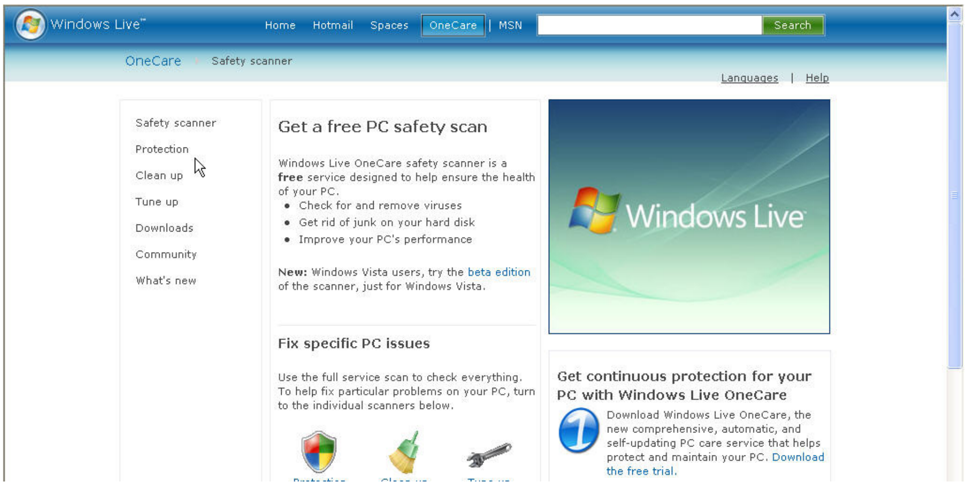
Note: Please check the file name carefully before you execute the delete action.

7. Run a full system scan to search the unknown virus files

At step 3, we have deleted some known virus files manually, but the variants of “Autorun virus” increase steadily, we suggest to run a full system scan to ensure that some unknown virus files can be undetected.

a. If you have installed antivirus software and able to connect to internet, please download the latest virus signature files. If your computer cannot connect to internet, you need to use another computer to the latest virus signature files of your antivirus software and burn to a CD-R. Then, restart the infected computer and boot up the windows, insert the CD-R, double click the files on the CD to install the latest virus signature files. After installation, run a full system scan. After finished, the scanning result lists out the virus infection status and recommended solution, follow the instruction to remove the virus files.

b. If you does not install antivirus software, we suggest you to run an online virus scanning tool, eg. Windows Live OneCare [See Figure 6]



Get a free PC safety scan

Windows Live OneCare safety scanner is a **free** service designed to help ensure the health of your PC.

- Check for and remove viruses
- Get rid of junk on your hard disk
- Improve your PC's performance

New: Windows Vista users, try the beta edition of the scanner, just for Windows Vista.

Fix specific PC issues

Use the full service scan to check everything. To help fix particular problems on your PC, turn to the individual scanners below.

Get continuous protection for your PC with Windows Live OneCare

Download Windows Live OneCare, the new comprehensive, automatic, and self-updating PC care service that helps protect and maintain your PC. Download the free trial.

[Figure 6]

Steps as below:

i. Connect to http://safety.live.com , at Windows Live OneCare safety scanner windows, select “Protection”. At “Protection Center”, click “Protection Scan”.

ii. A “Service Agreement” window describes the terms of usage, click “Accept” to agree terms.

iii. At "Install scanner", click "Install now", an information bar may be showed, you may see an "ActiveX installation notice" under Address bar, click "Install ActiveX". Then an "Internet Explorer warning windows" pop-up, ask you to install "Windows Live Safety Center Component", click "Install".

iv. Click "Launch scanner", a "Protection" windows pop-up, click "Next" to start download the scanning tools，it needs 10-15 minutes which depends on your connection speed.

v. After download, start to scan the storage device of your computer automatically.

vi. Scanning time depends on the size of hard disk and no. of files etc. Generally, it takes for 1-2 hours.

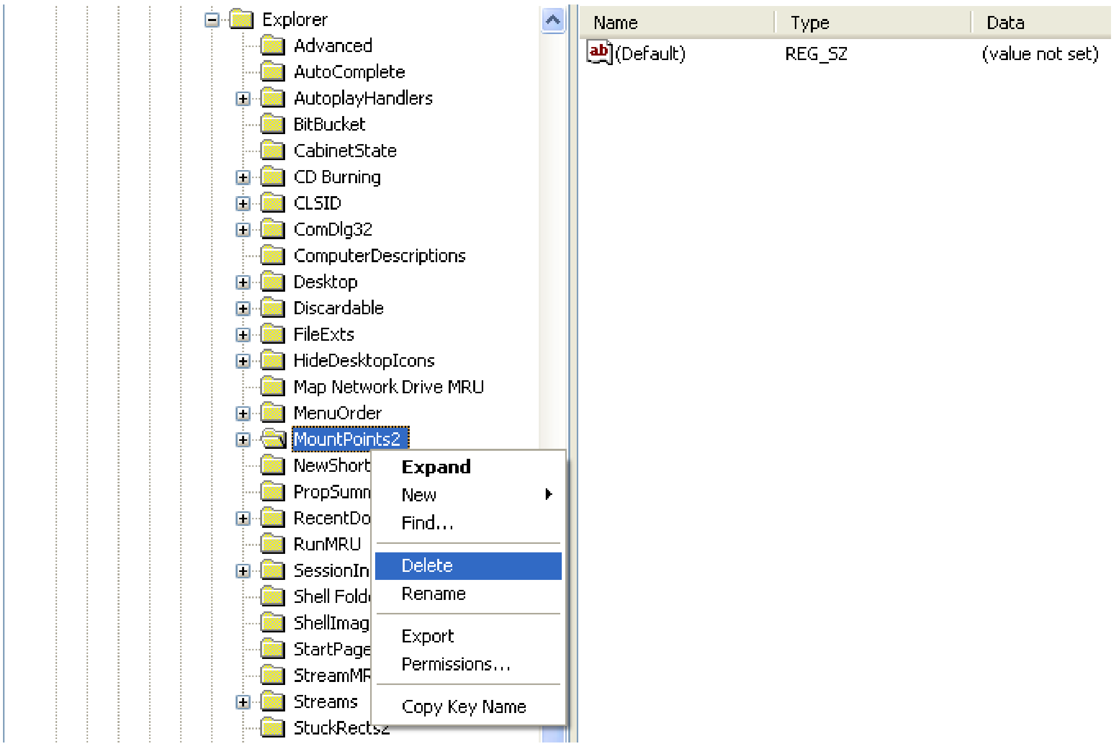
vii. After finished, the scanning result lists out the virus infection status and recommended solution, follow the instruction to remove the virus files.

8. Delete MountPoints2 registry key **[Updated on 22 January 2009]**

Microsoft Windows may cache the AutoRun information of previously connected devices to MountPoints2 registry key, even after you disable the autorun feature. When you connected an old devices to your computer, the system still executes the command stated in Autorun. For this reason, we recommend removing this cache on the infected computers by deleting the MountPoints2 registry key.

i. At “Start”->”Run”, input regedit and click “OK”, a registry editor window occurs.

ii. At HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 [See Figure 7]



Name	Type	Data
ab(Default)	REG_SZ	(value not set)

[Figure 7]

iii. Right-click “MountPoints2”, and then click “Delete”.

iv. A confirmation dialogue box “Are you sure you want to delete this key and all of its subkeys ?” prompt and then click “Yes” to confirm.

v. Restart the computer to let the system reinitialize MountPoints2.

9. Restore system restore function (restore step2, only apply to Windows XP and Windows Vista)

I. For Windows XP

i. Click Start.

ii. Right-click “My Computer”, and then click “Properties”.

iii. Click the “System Protection” tab.

iv. Uncheck the "Turn off System Restore" or "Turn off System Restore on all drives"

v. Click “Apply” and then click “OK” to confirm.

vi. Restart the computer.

II. For Windows Vista

i. Click Start.

ii. Right-click “My Computer”, and then click “Properties”.

iii. Click the “System Protection” tab.

iv. On “Available Disks”, check the Local Disk (Default is C).

v. Click “Apply” and then click “OK” to confirm.

vi. Restart the computer.

- End -