

I. Purpose:

All staffs are bound to obey the following Antivirus policy while using the Corporate's computer to prevent jeopardising the company's safety as a whole.

II. Scope:

This guideline covers and binds all CSCM Corporate's computer equipment and Intranet's equipment, including and not limited to personal computer, moveable equipment and server etc.

III. Policy:

1. All computers must install the stipulated Antivirus software. Update such software timely, and accept scheduled virus scanning. Do not close such software without permission.
2. Do not open email(s) from unknown sources and delete it immediately. Turn off the "Preview" function in email software, i.e. MsOutlook to prevent unintentional opening of email(s).
3. Do not use email software such as MsOutlook to accept emails from other software i.e. G-Mail or Yahoo Mailbox, by using Corporate's Personal Computer, to prevent virus invasion.
4. Do not install any paid copyrighted software from unknown sources, unless with application and permission of the company.
5. Do not turn on the "Share File" function. For business operation needs, obey application procedure and the Information System Department will set up the requested share and access function in File Server.
6. Do not download from non-corporate related Internet using Corporate's personal computer.
7. Do not use an USB, unless with application and approval obtained.
8. Turn off the "Auto-Sign in" function. Do not use blank, your name, easy combination, less-than-6-characters combination as password of personal computer.
9. All important information must be saved in File Server for managing and backup purpose.

IV. Enforcement:

All staffs are bound by abovementioned security policy regulation; or subjected to Personnel Section's Regulation in the event of breach.