I. Purpose:

In order to prevent the virus affect or attacks, all the CSCM staff's computers or equipment must comply with the company Antivirus Policy.

II. Scope:

This policy covers and binds all CSCM Corporate's computer equipment and server. Corporate computer equipment is classified into Office Automation (OA) Computer and Operational Technology (OT) Computer. OA Computer: Antivirus software is installed with scheduled virus scanning; OT Computer: some are NOT installed with Antivirus software or without auto-update, to maintain operation stability.

III. Policy:

1. All computer equipment is installed with stipulated software subject to scheduled scanning. Do not uninstall such software without permission.
2. In the event of computer equipment projects unusual situation or signal, "Reduce and Avoid" further virus outbreak as per the following steps:
   - Identify computer unusual situation: crashes, auto shut down, unusual running program, unusual messages etc.
   - Subsequent method: Disconnect network connection and shut down.
   - Inform: Inform Related Departments (OA Computer: contact Information System Department; OT Computer: contact Power & Process Information Section, Electrical Section#1 and Electrical Section#2).
3. Common unusual situation (for computer without Antivirus software):
   - Unusual auto shut down
   - Unable log in to system after restart
   - Unusual situation: i.e. crash after opening of certain program, file or link
   - Program running out of control
   - Unusual and unintended opening and running of unknown apps and webpages
   - Slow running of apps and webpage
   - Unusual situation after clicking in unknown webpage
   - Sudden internet slow connection
   - Received other staffs' email on notification of unusual account

   Immediately contact Information System Department, Power & Process Information Section, Electrical Section#1 and Electrical Section#2 for urgent rescue action.

4. Antivirus Software Warning and Action:
   - Quarantine
   - Remove
   - Block
   - Successful, no further action needed
   - Discovered virus and cannot be removed
   - Discovered virus, cannot be removed but quarantined
   - Encrypted
   - No action taken temporary

- No action taken on existing security concern
- Further action needed
- Discovered Virus, quarantine but unsuccessful delivery to Quarantine File
- Alert OfficeScan on virus attacked user. Restart to complete virus removal process.

Analyse with the help of installed Antivirus software to have preliminary inference. Information System Department will conduct monthly check and record to review such information security issue. In the event the immediate action has no avail (i.e. unable to delete, quarantine, no further action or virus outbreak), inform Information System Department, Power & Process Information Section, Electrical Section#1 and Electrical Section#2 for immediate action.

5. Subsequent Progressing Method

   In the event of virus attack, disconnect to internet, shut down, and inform Information System Department, Power & Process Information Section, Electrical Section#1 and Electrical Section#2 Person-in-Charge.

6. Classification of Jurisdiction
   - Information System Department: Under control of Information System Department on OA Computer
   - Power & Process Information Section, Electrical Section#1 and Electrical Section#2: Control Level 1, Level 2 and Level 2.5 OT Computer.

IV. Enforcement:

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