ANNEX A - Computer Preventive Maintenance Procedures

Introduction

In order to ensure that the PNP-owned computers and computer peripherals are well-maintained to support optimum performance and to reach their maximum life spans without any hassle, the following maintenance schedule and procedures must be observed religiously by members of the PNP organization.

1. Maintenance Schedule

Procedure Number	Procedure	Schedule			
		Daily	**Weekly**	**Monthly**	**Annually**
1	Cleaning the Computer's CPU Box				X
2	Cleaning the Monitor				X
3	Cleaning the Keyboard				X
4	Cleaning the Mouse				X
5	Running Disk Cleanup Utility			X	
6	Running Disk Defragmenter			X	
7	Updating the Anti-Virus and Running Virus Scan	X	X		
8	Updating the Operating System (OS)	*As prompted by the OS*			

2. Preventive Maintenance Procedures

a. Cleaning the Computer's CPU Box

Dusts may clog in your computer's CPU box, particularly at the power supply and cooling fans. When clogged with dusts, the fans will have difficulty in rotating and may slow down or stop that can cause your computer to overheat.

To dust-off the CPU box, follow the steps below:

1) Turn off the computer and unplug it from the power outlet.
2) Remove the case lid.
3) Using a can of compressed air, blow the dust from the power supply through the slit in the computer chassis (CPU box) from inside out so the dust will exit at the back. Use short bursts and keep the can upright and a few inches from the hardware. Next, blow the dust from the intake fan and each of the exhaust fans. Blow out any other dust you see that has collected inside the computer. Also, be sure to blow the dust from the air vents on the case lid.
4) Check all the plugs & cables to make sure they are fixed firmly.
5) Re-assemble the case lid and plug your computer back into the power outlet.

Aside from removing the dust from the CPU box, it is also recommended that you check all the cables and connectors to see if there is any that is loosened and needs to be fixed.

b. Cleaning the Monitor

1) For Non-flat panel monitors

Use the monitor cleaning product (spray and wiping cloth) that comes with the computer packaging. Do not spray directly onto the monitor itself, instead, spray onto the cloth and then wipe the cloth over the screen or monitor cabinet.

Monitor cleaning products are commercially available, be sure that the one purchased is meant for the type of your monitor.

2) Flat panel monitors

These monitors usually have plastic screens and other components that can be damaged by cleaning products that use chemicals (benzene, thinner, ammonia, acetone), abrasives, or compressed air. To clean this kind of monitor, lightly dampen a soft, clean cloth with water, and use that to clean the screen. The monitor cabinet can be cleaned with a cloth lightly dampened with a mild detergent.

c. Cleaning the Keyboard

Make sure your computer is turned off before you work on your keyboard.

You can use compressed air to blow debris out of your keyboard, or turn it upside-down and shake it gently. **Do not disassemble it**.

Cleaning materials such as pads or swabs that contain a cleaning liquid can be used on the keys and upper surface.

d. Cleaning the Mouse

Properly cleaning a mouse does not only avoid malfunction but will make it easier to use and prevent the cursor from "jumping around" on the screen due to dirty rollers.

1) For Mouse with ball/roller

a) Make sure the computer is turned off;
b) Remove the mouse from the computer;
c) Look for the product manual that comes with the mouse and follow the instructions how to do disassembly;
d) Clean the ball with clear tape;
e) Check the rollers inside and scrape off any alien items using a straightened paperclip;
f) Hold it upside-down and shake out dusts; and
g) Reassemble.

For more information, visit this website: http://www.wikihow.com/Clean-a-Mouse-Ball

2) For Optical Mouse

An optical mouse uses laser to track movement. It does not have a mouse ball or roller, hence, does not require the kind of cleaning that a

mouse with ball does. To clean it, simply wipe the glass on the bottom of the mouse that houses the laser using a smooth cloth (lightly damp the cloth when necessary to remove sticky dirt).

e. Running Disk Cleanup Utility

Use this procedure to clean a particular disk of the following **unnecessary files**: Downloaded Program files, Temporary Internet files, Offline webpages, Game Statistics Files, Recycle Bin, Setup Log Files, System error memory dump files, System error mini-dump files, Temporary files, Thumbnails, Per user archived Windows Error Report Files, Per user queued Windows Report Files and System archived Windows Error Report Files, in order to reclaim disk spaces used by them.

To do this, follow the steps below:

1) Open the *Windows Explorer*;
2) Right Click on the Letter of the Disk Drive that you want to clean;
3) Select *Properties*;
4) On the new screen, click the *Disk Cleanup* button;
5) Choose the types of **unnecessary files** that you wanted to get rid of by clicking the corresponding check boxes; and
6) Click the *Clean up system files* button.

Another way to do this procedure is to *Click on Start -> Programs -> Accessories -> Systems Tools -> Disk Cleanup*.
Note: You can further increase the available disk space in the computer by removing unnecessary program or application, particularly those that are "trial version" and have already expired. However, this may not be performed by a usual user if the computer is configured with restriction that prohibits access to program/application removal tool.

f. Running Disk Defragmenter

The Windows Disk defragmenter organizes files and data into areas that helps the computer run smoothly. It moves the frequently used files to an easy access area and the least used files, to the opposite. It also gathers fragmented files and groups them back together. In short, Disk Defragmenter consolidates fragmented files on your computer's hard disk to improve system performance. Follow the steps below according to the operating system of your computer:

1. For Windows XP

    a) Open *My Computer*;
    b) Right-click the local disk volume that you want to defragment, and then click *Properties*;
    c) On the Tools tab, click *Defragment Now*; and
    d) Click *Defragment*.

2. For Windows Vista

    a) Go to *Start Menu*;
    b) Click *All Programs*;
    c) Click *Accessories;*
    d) Click *System Tools*;
    e) Choose *Disk Defragmenter; and*

f) Click *Defragment Now* button.

3. For Windows 7

a) Open *Windows Explorer;*
b) Right click on the Letter of the Disk Drive to defragment;
c) On the newly opened screen, click the *Tools* tab;
d) Click the *Defragment Now* button;
e) Click the *Analyze Disk* button to do some fragmentation analysis on the disk; and
f) Click the *Defragment Disk* to perform defragmentation.

g. Updating the Anti-virus and Running Virus Scan

Doing the virus scanning regularly will keep the computer safe from known viruses, worms, Trojan horses, and other malicious software. The steps depend on the anti-virus software installed in your computer. It is highly recommended to scan the computer at least once a week.

However, the anti-virus program may not be able to detect a new virus. The reason for this is that, a new virus carries a signature which is not present in the old database used by the anti-virus software, hence detection is not possible. To help your anti-virus cope up with new viruses, upgrading its database is necessary at least weekly or, if possible, daily.

h. Updating the Operating System (OS)

Most operating systems require regular updating or installation of new patches to secure identified vulnerabilities that may be compromised by viruses, worms and other security threats.

The steps needed to conduct OS update depend on what operating system is installed in the computer. However, most latest versions of Windows, i.e., Windows Vista and Windows 7, have automatic OS update detector which prompts the user once new updates are available in the Internet site.

If you are using a different OS, please consult its documentation or browse the Internet for more information.

3. Miscellaneous

Aside from conducting preventive maintenance procedures, the computer user or operator is required to follow certain precautionary steps to ensure the security of the computer and its stored data.

a. Basic Security

Although, no one can secure a computer system completely, but chances of attacks to computer system can be reduced if the user or operator follows certain security principles. Listed below are some of the guiding principles that a computer user or operator must bear in mind in order to protect the machine from external threats:

1) Use strong passwords for log-on screen, and change it regularly (monthly or quarterly);

2) DO NOT share your password to other users. If more users are required to operate the computer or have access to an application, each should be given a user account and password;
3) Log-off from the active mode or activate the Screensaver with password protection before leaving the machine;
4) Regularly check if the computer is affected by a virus, spyware and/or adware by regularly using the virus and malware scan features of the anti-virus system;
5) Regularly update the operating system and all other programs like Adobe, Internet browser (such as Internet Explorer, Google Chrome, Mozilla Firefox, etc), and other applications;
6) Regularly back up important files;
7) Use encryption techniques in transmitting sensitive information either through e-mail or LAN communication;
8) If possible, use firewall and intrusion detection systems;
9) Turn off your system or disconnect from the Internet when not in use;
10) Ensure the physical security of all hardware used; and
11) Be aware of current security threats, vulnerabilities and attack techniques. Consult your IT Officer for more information about these.

b. Data Backup Checklist

1) Back up important documents, photos, videos, email messages, etc. to CD, DVD, or another external disk at regular intervals. When creating back-ups, it is not recommended to use thumb drive (USB drive) or flash card as these devices are easily destructible;
2) Keep multiple backup copies of important data;
3) Use encryption techniques to protect backup data;
4) If available, use the automated backup feature in the program or application as manually creating backups may result to human error;
5) Keep your backup in a safe place; and
6) Verify your backup process for its effectiveness.

c. Physical Security

1) Minimize the amount of paper and sensitive information left on desks after performing data encoding, report preparation or other similar tasks;
2) Lock these documents in cabinets;
3) Survey the building and deal with obvious problems;
4) Use strong locks for doors and windows;
5) If not officially required, do not bring home office laptops and other mobile devices that contain sensitive data or information; and
6) If not in use, make sure that the laptop is properly turned off and place it inside of a secured cabinet.