


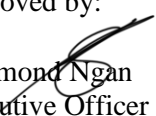
MITSUKOSHI MOTORS PHILIPPINES, INC.		
POLICY AND PROCEDURE		
POLICY TITLE :	COMPUTER SECURITY CHECKS	Ref. No.
DEPARTMENT :	INFORMATION TECHNOLOGY	ITD-15-12-0302
TO :	BRANCH MANAGER, AREA MANAGER	

OBJECTIVE

1. The objective of this document is to educate managers to conduct security checks on branch equipment, and ensure compliance of branch personnel of computer policies procedures contained in this document.
2. To ensure business protection from intrusive software such as computer viruses, worms, trojan horses, spyware, adware and the like.
3. To protect the company assets and information against corruption and ensure proper working condition of branches.
4. To ensure that personnel across branches are complying with IT rules and regulations.

POLICIES

1. Branch personnel are not allowed to use or install any prohibited application and software in their work computers, prohibited applications include but are not limited to:
 - 1.1.1. Games
 - 2.1.1.1. CD provided gaming software e.g. Internet, LAN, RPG, etc.
 - 2.1.1.2. Internet provided gaming software e.g. Mini-clips and Facebook Games.
 - 1.2.1 Downloading of Torrent, Limewire, BearShare, ARES, Internet Downloader Manager (IDM), etc.
 - 1.3.1 Software or Programs for customizing/upgrading windows, e.g. wall papers, screen saver, etc.
 - 1.4.1. Others
 - 2.1.4.1. Media and communication application
 - 2.1.4.2. Other prohibited application by the IT Department
 - 2.1.4.3. Systems/Application installed except for company
 - 2.1.4.4 Other Antiviruses except AVAST.

Prepared By: Suzelle Ngan Updated By: Suzelle Ngan		Approved by:  Richmond Ngan Executive Officer	Effective November 2015	Page 1 of 6
---	---	---	--------------------------------	-------------

2.1.4.5 Applications or other executable files that disables/destroys the network firewall restrictions.

2.2. Prohibited files

2.2.1. Unexpected Media Files

- 2.2.1.1. Video, Music, MP3, MP4, etc.
- 2.2.1.2. Pictures, logos, banners, etc.
- 2.2.1.3. Thumbnails, icons, etc.

2.2.2. Non-Microsoft Files, unknown type of file extension. The only file extensions allowed are;

- 2.2.2.1. DOC, RTF, XLS, PPT, MDB, RPT
- 2.2.2.2. Windows/Program Files
- 2.2.2.3. Executable Files set by the IT (Company Systems, Antivirus, Optimize Executable)

2.2.3. Internet Downloaded Files

2.2.4. Shared Files and Plug-Ins Data

2.2.5. Unauthorized Executable Files

1.2. Prohibited Internet Sites

- 2.3.1. Social Network Sites, e.g. Facebook, Friendster, Multiply, etc.
- 2.3.2. Internet Games and Pornographic Sites
- 2.3.3. Forum Sites
- 2.3.4. Any sites that have no relation to Company's operations


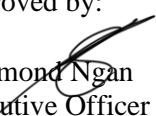
2.4. CD-ROM or USB device must be used or executed with the user's permission; it should be with the permission of the branch cashier or branch manager for branch employees. Further, these devices must first be scanned for any viruses before use or execution.

2.5. Sharing of system/computer user's name and password is strictly prohibited. In the event of discrepancies, the responsibility will fall upon the owner of the username in question. Therefore it is of every employee's best interest not to share their username and password.

All branch personnel must ensure that the area where the branch computer is located is kept in a restricted area where unauthorized person are not allowed to enter.

2.6. Only the IT Department administrator is allowed to modify the following systems and programs:

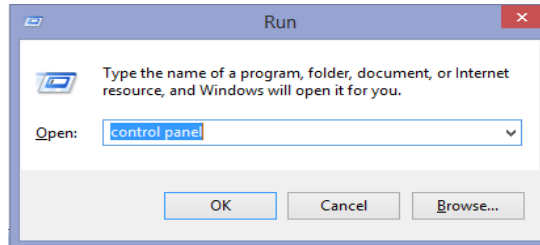
- 2.6.1. Firewall – reconfiguration or disabling the company firewall is strictly prohibited.
- 2.6.2. VNC software system - reconfiguration or disabling of the system is strictly prohibited.
- 2.6.3. Internal structure of the system set-up by the IT Department, e.g. BMS, Inventory system, LMS, HR system, etc.

Prepared By: Suzelle Ngan Updated By: Suzelle Ngan		Approved by:  Richmond Ngan Executive Officer	Effective November 2015	Page 2 of 6
---	---	---	--------------------------------	-------------

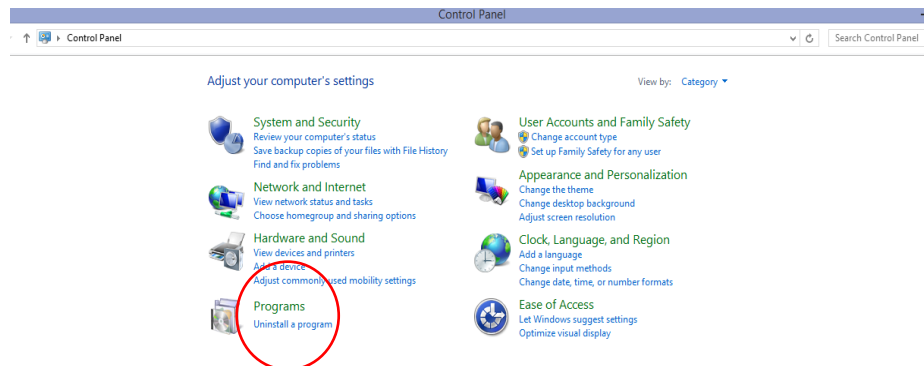
- 2.7. Each employee with assigned computer must have a confidential Username and Password. Only authorized head office personnel are allowed to make changes to employee username and password.

PROCEDURES


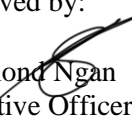
1. Open “Control Panel” in the desk top by pressing “Window Panel” and “R”; and the run box will appear.



- 1.1. Press “OK” and the “Control Panel” will appear.

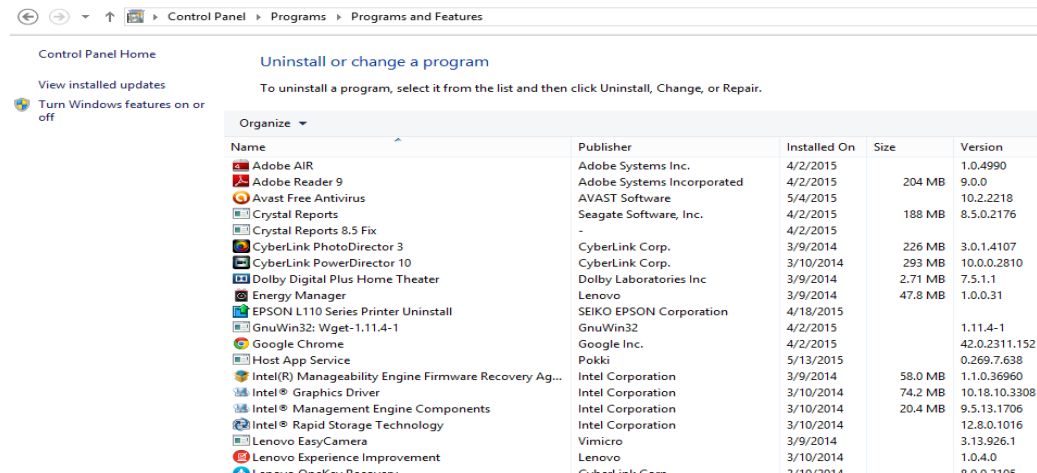


- 1.2. Proceed to “Program” and press “Add and Remove Program” or “Install Program”.

Prepared By: Suzelle Ngan Updated By: Suzelle Ngan		Approved by:  Richmond Ngan Executive Officer	Effective November 2015	Page 3 of 6
---	---	---	--------------------------------	-------------

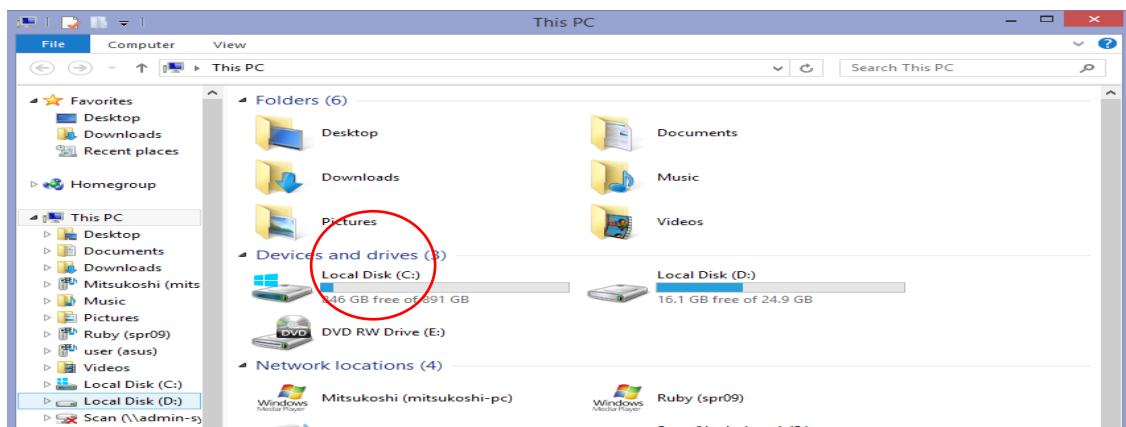
1.3. List of “Programs and Features” will appear. Check for illegal and unauthorized program; if illegal programs were found, notify HR Department in head office.

1.3.1. Discuss the matter to the branch manager or cashier and uninstall illegal program found in the branch desktop.



2. Proceed to “My Computer” or “This PC”.

2.1. List of Folders, Devices and drives and Network locations will appear. From the list of Devices and drives, choose and double click “Local Disk (C:)”



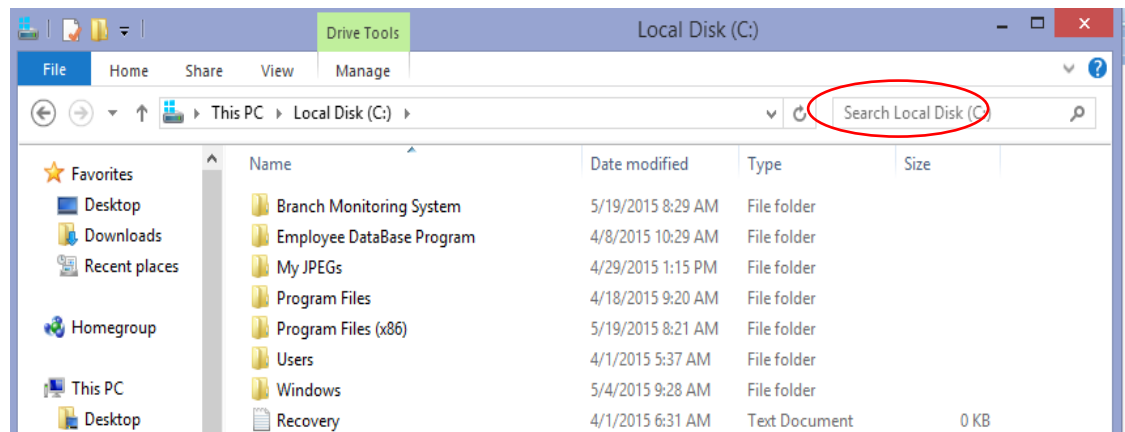
Prepared By:
Suzelle Ngan
Updated By:
Suzelle Ngan

Approved by:
Richmond Ngan
Executive Officer

Effective
November 2015

Page 4 of 6

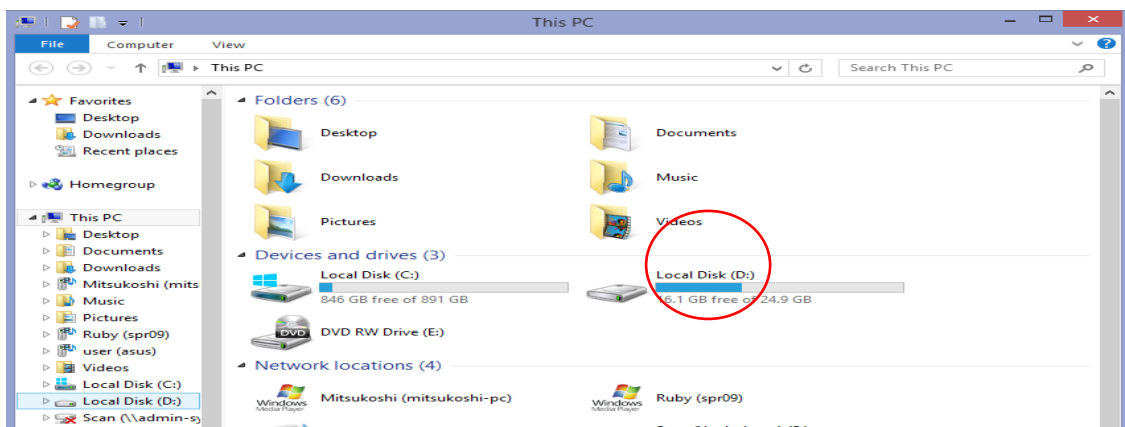
2.2. The “Disk (C:) will appear.



2.2.1. In the “Search Local Disk (C:)” in the right hand portion of the “Local Disk (C:), search for illegal

- 2.2.1.1. *.mp3
- 2.2.1.2. *.mp4
- 2.2.1.3. *.flv
- 2.2.1.4. *.mov
- 2.2.1.5. *.avi

2.3. After checking “Local Disk (C:)” proceed and check Disk D by double clicking “Local Disk (D:)”.



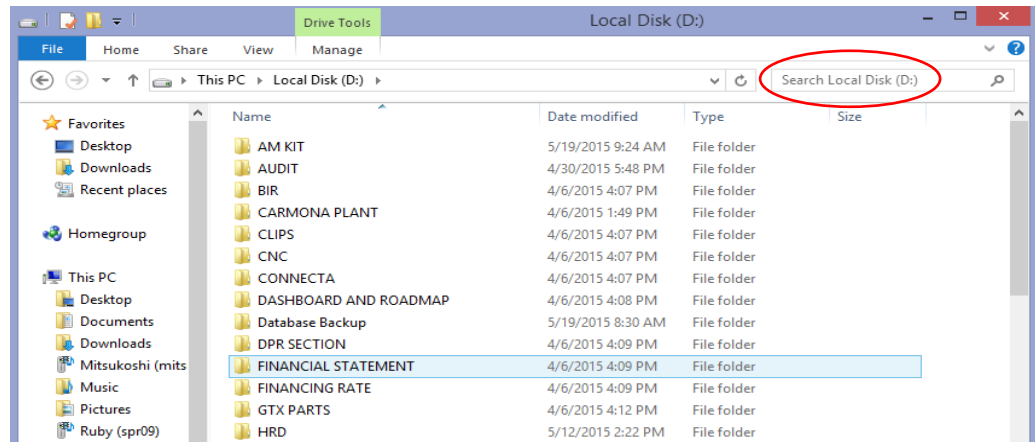
Prepared By:
Suzelle Ngan
Updated By:
Suzelle Ngan

Approved by:
Richmond Ngan
Executive Officer

Effective
November 2015

Page 5 of 6

2.3.1. The “Disk (D:) will appear.


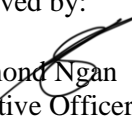


2.2.1. In the “Search Local Disk (D:)” in the right hand portion of the “Local Disk (D:), search for illegal or unauthorized download.

- 2.2.1.1. *.mp3
- 2.2.1.2. *.mp4
- 2.2.1.3. *.flv
- 2.2.1.4. *.mov
- 2.2.1.5. *.avi

3. If there are any illegal or unauthorized download found during the checking of drives C and D in the branch computer, document and send to HR. Ensure to include the following details:

- 2.2.1.1. Name of Offender
- 2.2.1.2. Screenshots of Files
- 2.2.1.3. Branch

Prepared By: Suzelle Ngan Updated By: Suzelle Ngan		Approved by:  Richmond Ngan Executive Officer	Effective November 2015	Page 6 of 6
---	---	---	--------------------------------	-------------