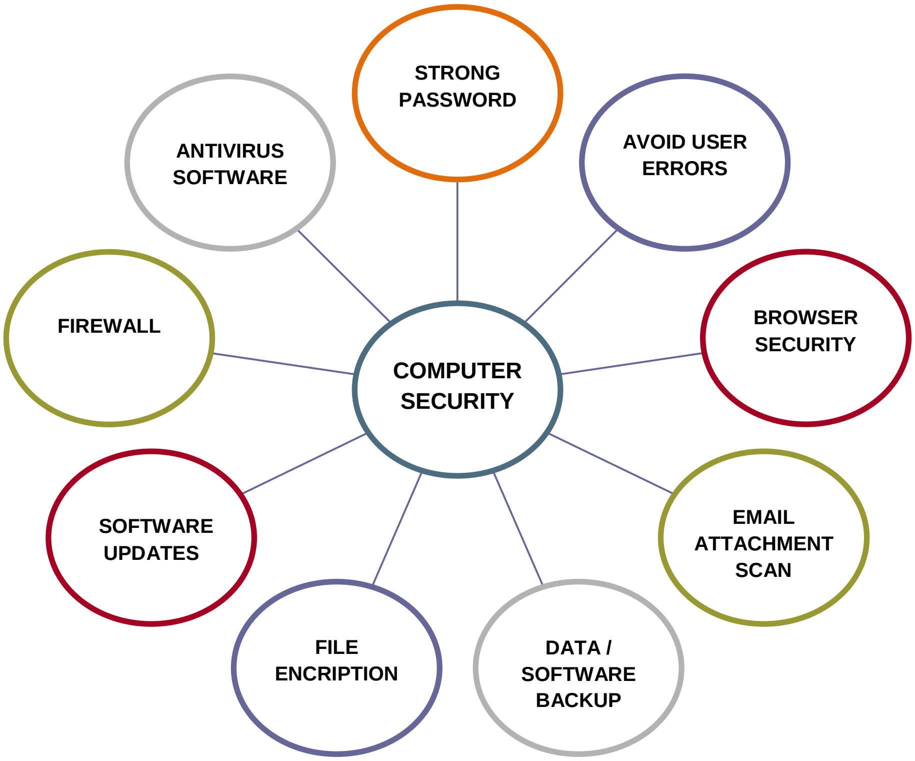
Computer Security Manual
for
Students, Faculty, and Staff



(Ravi K. Walia)
Assistant Professor & Incharge
Computer & Instrumentation Centre
Dr. Y. S. Parmar University of Horticulture & Forestry,
Nauni Solan INDIA (HP)

Preface

This document has been prepared for students, faculty, and staff at Dr. Y. S. Parmar University of Horticulture & Forestry, Nauni, Solan (HP) India. Specific instructions in this document apply to licensed versions of Windows Operating System, although many suggestions can apply to other operating systems and computing platforms. The retired versions of Windows are no longer updated with security patches, so they cannot be secured against hackers and malware and represent a threat to other computers on the campus wide local area network. If your computer runs one of these outdated operating systems, you must upgrade immediately to supported version of window and install the latest Service Pack to ensure the security of your data as well as campus network.

Personal Computer has no inherent security for users with confidential data hence they are the biggest threat to computer security. The data stored in PC is vulnerable because anyone can walk up and turn the switch ON and access information. Security issue became more important, when your computer is connected to the Internet, because hacker can hack your computer. When a computer is compromised, an individual who controls it may use it for organized attack on the other computers, websites or entire network.

In a large network such as campus wide network where large numbers of users are using the system and hence more the entry points which can make attacking the system easier and thus more potential for fraud and abuse. Wireless access, use of laptops, smart phones and malicious software make security issue even more difficult.

Computer users need to understand computer security, just as drivers need to understand the “rules of the road” to avoid unpleasant results. Whenever computer security is compromised it can result in its improper functioning, data/ information loss, identity theft, embarrassment and financial loss. To secure computer user must keep the computer up to date, use strong password and use a good antivirus and antispyware software.

Computer Security is not only IT/Computer Science department responsibility but individual responsibility also. Effort has been made by installing UTM (Unified Threat Management) System to cover all security vulnerabilities in the system. “Required computer maintenance” used to mean “defragment your hard drive and check for viruses”. These two duties are still required to maintain your computer, but your maintenance responsibilities have expanded. Take little more care and enjoy safe computing.

Table of Contents

Topic Page

INTRODUCTION

Security: Data or information security is the protection of data against accidental or intentional destruction, discloser or modification. Computer security refers to the technological safeguard and managerial procedure which can be applied to computer hardware, software and data to ensure that organizational and individual privacy are protected.

If your computer is not secured, it will get compromised—and when it gets compromised, it must be formatted and reloaded before you can trust its security again. It is time consuming and inconvenient to reload a computer from scratch. So keep your computer secure so that it does not need to be reloaded.

Breached of Security: Some of the ways/ manners in which data loss or manipulation can occur are:

- Media Theft of PC and: A smart person with a false calling card can take away the PC for repairs and of course never show his face again. However electronic media like CD-ROMs, DVD-ROMs and Pen Drives are slightly safe as it is far easier to lock up in safe place.
- Damage Due to Breakage: It is hard to visualize dropping PC's but can happen if they are shifted from one place to another. More likely is that something may get dropped on the PC resulting in damage. Damage can also occur due to natural causes such as storms or flood or due to electrical and other fires.
- Environmental Damage: The manufacturer recommends some environmental conditions like temperature and humidity ranges, voltage limits, dust microns limits etc. If the conditions in your office remain outside these limits the PC and media are likely to get damaged.
- Inadvertent Corruption/ Loss: This can occur due to
    - Usage of inferior media: if sub-standard media is used as it would be generally cheaper but after using it for some time it may develop faults and data stored in it may become unusable.
    - Erasure of File: Files may get erased from the media due to incorrect action by the operator. Corruption may occur due to the PC being subjected to frequent power failure, wrong programming technique or defective software

- Environmental Losses: Excessive dust or humidity can result in corruption of disc surface or read/write head resulting in loss of data.
- Malicious damage/ Leakage: It is not necessary that this would be done by outside, it is equally possible that some unhappy or impish insider may wreck havoc.
- Unauthorized Access: Due to human tendency and / or curiosity for trying to look at things they should not or need not. Unauthorized information can be accessed and copied for malafide use.
- Modification Erasures etc: The person accessing data file may be authorized to read the data only but he would like to alter, modify or erase the data by writing in to the file.
- Computer Viruses: This is the latest threat to computer users. These can introduced deliberately or unknowingly by anyone at anytime and the consequences to the user would be equally disastrous. Have you ever picked up a cold or the flu from another human? Probably. You then spread it to two or three other people through touch or association. Those people spread it to two or three more people each. Soon it seems that everyone on the campus or at family is sick. That is how computer viruses are spread. You copy a file from an infected source, use the file and maybe sent it to friends or associates. The virus is now on your computer and spreads to files other than the original. You then send the same or even a different file to a few friends and their computer are infected. Smart phones are also now being targeted as a way to spread viruses. The problem created by viruses include:
    - Destruction of file allocation table – the user loses everything on the media
    - Erasing of specific programs and/or data on discs
    - Alter contents of fields in a file
    - Suppress execution of RAM resident programs
    - Destroy parts of program/data held on disc by creating bad sectors.
    - Reduction of free space on disc
    - Formatting of discs or tracks on discs in different way.
    - Overwriting of entire disc directories
    - Hang the system at periodic intervals so that keyboard become inoperative
    - Automatic copying of results obtained by other programs into some designated disc area.
- Data Tapping: In large computer system or when system is on network data has to travel over communication lines. Any person trying to get access to data can intercept the

traffic on the circuit by tapping in to the cable at some convenient point. A person can listen to the traffic on a line even without physically connecting in to it. Thus data following over communication lines is ever susceptible to “eavesdropping”.

Security threats to your computer can be classified in three groups:

- **Hackers,** who try to break into your computer without your knowledge or permission. They may also steal your data or use your computer to commit a crime by controlling your computer from remote location.. In any case, hackers are unethical people who should not be trusted.

- **Malware** (malicious software), which comes in many forms: viruses, worms, Trojan horses, scripts, rootkits, adware, and spyware. Malware can take control of your computer without your knowledge or permission, delete your data, send your data to an unauthorized recipient, or cause your computer to attack other computers.

- **User error**, which includes ignorance, laziness, and wrong command/instruction. Users must keep their computers up to date, use passwords whenever available, and ensure the passwords are not guessable.

SECURE YOUR COMPUTER

You must perform the following tasks to ensure the proper security and operation of computer:

- If computer runs Windows, follow the directions in this document to secure your computer. If your computer runs any older version of Windows which is not supported by Microsoft, upgrade immediately as old versions cannot be secured against modern security threats.

- Protect your computer with strong passwords. Leaving password fields blank or using default passwords will get your computer compromised very quickly.

- Use system password on your computer.

- Microsoft Update must be run daily to ensure that all Critical Updates have been applied to your computer. You can configure this utility to update your computer automatically.

- Use antimalware software, never turn off or disable antimalware software. Update antimalware definitions daily and scan all your files at least weekly to protect against malware that can destroy your data and render your computer useless.

- Firewalls should be used on any computer that connects to a network/Internet. Windows operating system contain a built-in firewall.

- Whenever you leave your computer, lock it. Press the CTRL, ALT, and DEL keys simultaneously, then release them and choose “Lock Computer.” All current processes and active programs will continue to run, but unauthorized individuals can’t use your computer until you login again.

- Use a password-protected screen saver & configure it to blank your screen after 10 minutes of inactivity. Use only screen savers included in your Windows operating system.

- Turn off your computer if it will be idle for more than a few hours, especially if it will be idle overnight. A computer can’t get compromised while it’s turned off—and it doesn’t waste electricity!

Passwords

- Use passwords whenever possible.
    - Never use a blank password.
    - Change all default passwords immediately.
    - Use strong passwords
- Create strong passwords by following these guidelines
    - at least 8 character long and combination of numbers and letters
    - mix of upper case, lower-case letters and special characters
    - Don’t use dictionary words, your account name, proper names.
- Keep passwords secret.

  - If someone else uses your userID and password, you will be held accountable for their actions.
  - Don’t write down your password
  - Never reveal your password to anyone
  - When using a computer or accessing a website, never use any option that offers to “save my password for the next time,”“automate my login”.
- Change passwords at least every 90 days.
  - Don’t re-use old passwords.
  - Don’t use the same password for multiple systems.

Software Update

- Patch your software (operating system and applications). Hackers will use newly-discovered security flaws. Automate the checking for updates of operating system and applications on a daily basis. Apply security patches as soon as they become available.

- Never open any e-mail attachment, regardless of its source. Save the file to your computer’s hard drive and scan it for malware.

- Avoid software you don’t need. If you don’t need it, don’t install it. If you’ve installed it and you don’t use it, uninstall it, such software are Add-on browser toolbars, Remote control and remote access software, Instant messaging software, chat software, Web server software and Password-caching software etc.

Secure Your Browser

- Block the “popup” in browser to prevent popup windows from cluttering your screen.
- Never use an option to “remember my password the next time.”
- Turn off the option to save encrypted web pages to your hard drive, since it also require password which also get saved to your hard-drive.
  - In Internet Explorer go to Tools, Internet options and select advanced tab in security section
    - Select the box in front of “Do not save encrypted pages to disk.”
    - Select the box in front of “Empty Temporary Internet Files folder when

browser is closed."

        - Deselect the box in front of "Use SSL 2.0" The boxes to use SSL 3.0 and TLS 1.0 should be checked.
    - In Firefox go to Tools, Options, privacy
        - In the History section select "use custom setting for history" and deselect all options.
        - In the Cookies section, use the drop-down box to keep until "I close Firefox."
        - In the Passwords section, deselect all choices

Security for Wireless Networking

Wireless networks should never be considered secure. You need to take extra security precautions when using a wireless network, especially if it's a public "hot spot" located in a hostel, hotel and cafeteria or cyber café.

- Disable Wi-Fi ad-hoc mode. Wi-Fi runs in two modes: infrastructure mode (when you connect to a network) and ad hoc mode (when you connect directly to another PC). If you've enabled ad hoc mode, someone near you could establish a connection to your computer without your knowledge, and they'll have free reign on your PC. To turn off ad hoc mode:
    - Right-click the wireless icon in the System Tray.
    - Choose Status.
    - Click Properties.
    - Select the Wireless Networks tab.
    - Select your current network connection.
    - Click Properties, then click the "Association" tab.
    - Uncheck the box next to "This is a computer-to-computer (ad-hoc) network."
    - Click OK until the dialog boxes disappear.
- Encrypt your sensitive data using Winzip software on a computer that will be connected to a wireless network. If your data is encrypted and somebody gets into your PC, they won't be able to read or alter any of your data.
- Use a personal firewall. Windows Operating System contains a firewall
- Turn off file sharing by Right-click on the drive or folders you normally share, Choose "Sharing and Security," and uncheck the box next to "Share this folder on the network."

- Ensure the network is legitimate.
- If you want to work offline, disable your wireless adapter.
- Look over your shoulder. Advanced techniques aren’t required for someone to steal your user name and password
- Never leave your laptop alone.

Responsibility for security rests with everyone connected to the network.

Unified Threat Management (UTM) System has been installed in the campus network. UTM technologies help organizations by providing all the security tools available in one comprehensive package to ensure they cover all security vulnerabilities in the system. It includes Firewall to prevent unauthorized users from accessing internal networks. Firewall protects the internal system by monitoring packets for the wrong source and destination. UTM gateway level antivirus prevents viruses and malware from the internet. UTM Intrusion detection system monitors the most vulnerable points in a network to detect and deter unauthorized intruders. Individual user must take care of the following points:

- Never install pirated software.
- Never install software from an unknown source
- Use your locks on doors, drawers, and computers.
- Never reveal your password to anybody, including your superiors.
- Never reveal confidential information.
- Don’t get fooled by the following security fallacies:
    - “I run antimalware software, so I’m secure.” Antimalware software doesn’t protect against hackers exploiting un-patched security flaws in your software.
    - “I run a firewall, so I’m secure.” Firewalls can’t protect your computer if your operating system and applications don’t have all available patches installed.
    - “I don’t care about security because I backup my data daily.” That may be convenient for you, but what happens when your computer gets compromised and attacks other computers.

SECURE YOUR DATA

Data Storage Guidelines

Users are responsible for data stored in the computer and any consequences arising from its misuse. Computers can store vast amounts of information and if it crash you may lose all the data. If you backed up data you can reload the data on the computer otherwise you have to recreate the entire data from scratch. Some time before crash the computer got hacked and someone take control of your computer and access all your files and important information store in these files such as bank accounts, credit cards number personnel information and then it crashed, hence follow these guideline:

- Backup your data daily or frequently
- Store your backed-up data securely
- Deleted data may be recovered but the process is complex, expensive, and rarely recovers all deleted data.
- Sensitive data should be encrypted.
- Store data on secure server or external disk
- Don not store data on laptop or workstation
- Physically secure any data storage device that can be easily moved.
- Email is not secure, so you should not send sensitive data via email. If you must email sensitive data, it should be encrypted.
- Ensure that all data is wiped (not just deleted) from your computer before it is transferred to someone.

Data Encryption

Encryption is a method of scrambling data so that only someone who possesses the appropriate password or “key” can access the information. WinZip application compress the size of data files. The licensed version, named WinZip Pro, can encrypt files using 256-bit AES encryption. If you have sensitive data stored on PC or laptop, you should encrypt the sensitive data to protect it from unauthorized access or theft.

- Sensitive data stored on flash drives/ pen drives should be encrypted.
- Email is not considered a secure method of communication. However, if you must send sensitive information via email: encrypt the data and send as an attachment and send password to decrypt by separate mail.

UPDATING MICROSOFT SOFTWARE

Older versions of Microsoft Windows are no longer supported by Microsoft and cannot be secured against modern security threats. If your computer runs any of these older versions of the operating systems, you need to upgrade to the supported versions of the Windows immediately. The following guidelines apply to computers running Windows vista & Windows 7.

Update Microsoft Windows OS

- Exit all applications except your antivirus software.
- Click Start button and click all programs
- Select “Microsoft Update” or “Windows Update from the Start Menu. This will connect you to the Microsoft website.
- When the Microsoft website opens, you may be required to install software required to access the site. Select “Yes” to install it.
- Install the latest versions of Internet Explorer and Media Player.

Automating Windows Update

- If you use Windows vista, set your computer to update automatically as follows:
    - Click start button and in the search box enter the words "Windows Update" without the quotes.
    - Click on the option labeled "Change Settings"
    - select "Install update Automatically” and select a time the updates should be installed
- If you use Windows 7 set your computer to update automatically as follows:
    - Open the Start Menu, then select “Control Panel”
    - In Control Panel, select “Windows Update, then select “Change Settings””
    - Choose “Install updates automatically” and select a time the updates should be installed.
    - Select the checkboxes for “Recommended updates,” “Who can install updates,” “Microsoft Update,” and “Software Notification.” Click the “OK” button.

WHEN ANTIMALWARE SOFTWARE DETECTS MALWARE

You must ensure that the latest version of your antimalware program is installed on your computer. Antimalware programs are normally updated as soon as security vulnerabilities are discovered. The newest version of the program is the most secure. The antimalware program on your computer will communicate with you—pay attention to these messages. Ignoring this vital information can result in loss of all your data

Appropriate Responses to Notices

- Retrieving email. If the notice states, “Quarantine successful,” your antimalware program has prevented the malware from reaching your computer. Notify the person from whom you have received infected email.
- Installing new antimalware definitions. Your computer is infected by a new form of malware that your old definitions did not protect against
- Manually scanning files on your hard drive. Your computer was infected in the past by malware that arrived before updated virus definitions that could recognize it. The new virus definitions may be able to fix the infection.

Malware Types

- Virus: A self-replicating program, often written to cause damage or mischief, which inserts itself into a software application without leaving any obvious sign of its presence. Your computer can pick up a virus when you copy an apparently normal file from a diskette, CD, DVD, or memory stick, when you open an infected email attachment, or when you download an infected file from the Internet.
- Worm: Like a virus, a worm is a self-replicating program, often written to cause damage

or mischief. Unlike a virus, a worm is self-contained and does not need to become part of another program to propagate itself. Instead a worm infects the operating system, acts like a program in its own right, and spreads via the network.

- Trojan horse: A malicious program that appears to be innocuous or even beneficial, but conceals other malware that can compromise the security, data, and proper functioning of your computer. Trojan horses spread via the network and are sometimes referred to as "network viruses."
- Spyware: Programs that scan systems or monitor activity and relay information to other computers or locations in cyberspace. The information that may be actively or passively gathered and disseminated by spyware may include passwords, log-in details, account numbers, personal information, individual files, or other personal documents. Not all spyware is damaging to a computer system. It is a popular method for some websites to monitor how users navigate through a site, providing critical information that the web designers and developers can use to improve the site.
- Adware enables delivery of advertising content to you through its own or another program's interface. Adware may gather information from your computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer or other locations in cyberspace. Adware can be downloaded from web sites (often in shareware or freeware), email messages, and instant messenger programs.
- Backdoor: Software that bypasses normal authentication methods, such as a username and a password, and allows unauthorized people to access and control your computer without your knowledge.
- Blended threat: An attack on your computer from the network specially crafted to maximize the severity of damage and speed of infection by combining several kinds of malware.
- Keylogger: Spyware that records your keystrokes and sends the information to someone else without your knowledge. Keyloggers are often used to gather email and online banking usernames and passwords as a prelude to identity theft.
- Rootkit: Hides files or processes running on a computer, rendering them difficult to detect and remove.

How to Avoid Malware Problems

The most important component of malware protection is *you*. Use safe computing practices to protect your computer and its contents.

- Keep all software up-to-date, especially your operating system, browsers, and antimalware applications.
- Turn off your computer if you are not using it. If your computer is turned of It can't get infected by malware or hacked.
- Backup your data every day or weekly.
- Use the latest version of antimalware software with the latest version of the virus definitions.
- Never open any e-mail attachment, regardless of its source. Save the file to your computer's hard drive and scan it for viruses.
- Scan all files downloaded from the Internet for malware before you use them.
- Don't use peer-to-peer (P2P) file sharing software, which is inherently insecure and can share the entire contents of your hard drive.
- Don't click on anything inside a pop-up window to close it. Click on the "X" in the upper-right-hand corner to close the pop-up window.
- Adjust your browser to block pop-up windows.
- Don't click on links within pop-up windows—they may install spyware on your computer.
- Beware of "free" downloads that may install software on your computer without your knowledge or permission.
- Don't use add-on menu bars in your Internet browser.
- Don't use third-party search engines for your hard drive.
- Don't use shopping programs.
- Don't use any program that offers to save your userids or passwords.

INDICATIONS WHEN COMPUTER IS COMPROMISED

Your computer can be compromised by a hacker or by malware without human intervention. In either case, something malicious has been done to your computer without your knowledge or permission. Indications that your computer may be compromised:

- The computer became very slow. It takes longer to start than it used to and applications open slower than they used to.
- The computer locks up or shuts down unexpectedly.
- Your Internet connection slows down.
- Pop-up windows appear, but you didn’t open any application.
- The hard drive activity light continues to blink continually.
- The hard drive is full.
- Your antimalware program stops working.
- You can’t connect to antimalware sites on the Internet.

Running certain types of software such as peer-to-peer file sharing software, Chat or Instant Messaging software, Search assistant software, Internet-based games greatly increases the probability your computer will get compromised.

When Computer is compromised? (or you suspect it might be compromised)

Take the following steps

- Disconnect the compromised computers from the network (disconnect network cable, deactivate network port).
- Take the backup of important data
- The compromised computer’s hard drive should be formatted
- Reload the Windows Operating System
- Reload all software, especially service packs, security patches, and antimalware software.

COMPUTER CRIME

Computer crime is a growing national and international threat to the continued development of e-business and e-commerce. The following are the best known computer crimes

Computer as targets of crime

- Breaching the confidentiality of protected computerized data
- Accessing a computer system without authority
- Knowingly accessing a protected computer to commit fraud
- Intentionally accessing a protected computer and causing damage, negligently or deliberately
- Knowingly transmitting a program, program code or command that intentionally causes damage to a protected computer
- Threatening to cause damage to a protected computer

Computer as instruments of crime

- Theft of trade secrets
- Unauthorized copying of software or copyrighted intellectual property, such as article, books, music and video
- Schemes to defraud
- Using e-mail for threats or harassment
- Intentionally attempting to intercept electronic communication
- Illegally accessing stored electronic communications, including e-mail
- Transmitting or possessing child pornography using computer

It is very difficult for our society and our government to keep up with the rapid change in the type of computer crime being committed. Many laws have to be rewritten and many new laws must be implemented to accommodate the changes.

IDENTITY THEFT

The fastest growing crime on the Internet is identity theft. Guard your personal information as if it's your most important asset. Even though identity theft is most likely to occur in an offline environment, once your personal information has been stolen it's easy to use it in an online environment. If someone steals your personal information they can gain access to your assets within no time. They can buy cars or any other valuable item in your name and you have to prove that you did not do it.. The biggest risk of identity fraud is from people who know you, people who are close to you. There are many precautions people can take to help prevent identity theft.

- One way is to scrutinize emails or phone calls that ask for your personal information or financial account information. No legitimate financial institution will ever send an e-mail requesting you to supply your account information. You should ignore and delete these e-mails immediately.
- Use strong passwords. If someone guess your weak password and breaks into your account (email, bank, credit card), you have nobody to blame except yourself.
- When using computer or accessing website, never use an option to "Remember my password the next time". This option will store password in a standard location on the computer, which is the same as writing it down just as bad. If your password is stored, it can be found and used against you.
- Expect someone to read any document you discard. Shred all discarded document using paper shredder.
- Beware of Shoulder surfers – people who look over your shoulder at your computer keyboard or monitor. They can note down your id and password If they have camera or camera equipped cell phone they can record the keystrokes of your ID and password and your personal information displayed on the monitor.
- Make a photocopy of your important documents such as credit card, license and all the account numbers and phone numbers to call and cancel. Keep the photocopies in a safe place.
- Do not use public computer for e-commerce, to check your emails or access your bank account.

SYSTEM MAINTENANCE FOR THE PC

Use the following windows utilities to improve the speed of PC

Check Disk

Run Check Disk weekly to check your hard disk for damaged files that degrade performance. It must be run separately on each partition on your hard drive, as follows:

- Double-click the My Computer icon
- Right click the appropriate Drive icon, select Properties, select the Tools tab.
- Click the Error Checking button.
- Click the Check Now button.
- In the Check Disk Options, select both options
- Click the Start button to begin checking the hard drive.

You may need to reboot your computer for the disk to be checked.

Disk Defragmenter

Run Disk Defragmenter weekly to increase system speed. It must be run separately on each partition on your hard drive. To start the utility:

- Double-click the My Computer icon.
- Right click the appropriate Drive icon, select Properties, select the Tools tab.
- Click the Defragment Now button.

This utility will require several minutes to defragment each partition on your hard drive.

Disk Cleanup

Run Disk Cleanup utility monthly to increase system speed. Disk cleanup removes number of unnecessary files from hard disk to free up disk space and help your computer run faster. It removes temporary files, empties the Recycle Bin, and removes a variety of system files and other items that you no longer need.

It must be run separately on each partition on your hard drive. To start the utility:

- Double-click the My Computer icon.
- Right click the appropriate Drive icon, select Properties, select the General tab.
- Click the Disk Cleanup button.

This utility will calculate the total disk space that can made free. Select using check box the types of unnecessary files you want to remove and click ok.

QUICK REFERENCE

Take the following steps to secure computer from virus

- Always update your antivirus software with latest patches from the vendor services
- Scan the system with anti-virus software regularly to avoid virus
- Take backup of your important data periodically
- Also use anti-spyware, anti-malware and anti-adware tools
- Always update the operating system with latest patches.

Take the following steps if computer is infected with virus

- Remove the network connection
- Take backup of data
- Install anti-virus software in your system and scan it
- Restart the system with network connection and update the antivirus.
- Once again scan the system.

Take care of following Preventative Maintenance Tips

- Always keep your operating system and programs up-to-date.
- Install an antivirus and antispyware program that automatically scans for viruses when the system boots.
- Update the virus/spyware definitions daily to ensure your system is protected against the latest threats.
- Do not download any files from the Internet unless you are certain the source is not transmitting a virus to you, or that the files are spyware-free.
- Do not use any storage media that has been used in another computer unless you are certain the other computer is free of viruses and will not pass the virus on to your system.
- Never open email attachments from people you don't know; and don't open any file attachment that ends in '.exe.
- Download the email attachment file and then scan with anti-virus software.
- Keep all document and other software disks of PC in safe place.
- If operating system disks are not provided with the PC, create system restore disks, which can be used to restore your system when there is some problem.
- Backing up your data periodically will protect your data and make it easier to recover from a disastrous event.
- Always keep two-three backup copies of important data on different media.
- Always Use UPS with good backup time to protect PC form electrical surges as well as to avoid problem of windows, application software and data corruption.