Safe Computing:
Virus Safety, Backing Up Data and Using Network Drives
# TABLE OF CONTENTS

Chapter 1  
Virus Safety ........................................................................................................ 1  
A. General Information on Computer Viruses ......................................................... 1  
B. SOPHOS Anti Virus - SAV ..................................................................................... 1  
C. Using Sophos ....................................................................................................... 2  
D. Updating SAV at Work, using Novell ................................................................. 3  
E. Installing SAV at Home, or on campus without using Novell ......................... 3  
F. Updating SAV at Home, or on campus without using Novell ......................... 3  
G. Email Virus Information ....................................................................................... 4  
H. Disinfecting at Home .......................................................................................... 5  
I. Network Vulnerability ......................................................................................... 5  
  I. Shared Files and Folders ...................................................................................... 5  
  II. Open Ports ......................................................................................................... 5  
  III. Spyware ........................................................................................................... 5  
  IV. Firewalls ............................................................................................................ 6  
  V. Spam ................................................................................................................... 6  
  VI. Hoaxes ................................................................................................................ 6  
  VII. Phishing ............................................................................................................ 6  
J. Responsible Computing ........................................................................................ 7  

Chapter 2  
Smart Browsing ....................................................................................................... 9  
A. Windows Updates ................................................................................................... 9  
B. Cookies .................................................................................................................. 9  
C. Saving Internet Passwords ................................................................................... 10  
D. Popup Blockers ..................................................................................................... 12  
E. Temporary Internet Files ...................................................................................... 12  
F. Cache Clearing ....................................................................................................... 12  

Chapter 3  
Password Safety ....................................................................................................... 15  
A. General Information on Passwords ...................................................................... 15  
B. Changing your Passwords .................................................................................... 15  

Chapter 4  
Network Drives ....................................................................................................... 17  
A. General Information on Network Drives ............................................................ 17  
  I. Benefits of using a network drive ........................................................................ 17  
  II. Network Drives at the University of Regina ..................................................... 17  
  III. Shared Documents Folder ............................................................................... 17  
  IV. Files and Folders on Local Disk (C:) ................................................................. 17  
  V. Files and Folders on Local Disk (D:) ................................................................ 18  
B. Access to Network Drives .................................................................................... 18  
  I. I:\drive ............................................................................................................... 18  
  II. T:\drive ............................................................................................................. 18  
C. Saving Files to a Network Drive .......................................................................... 18  
  I. Copying existing files to a Network Drive .......................................................... 18  
  II. Saving new files directly to a Network Drive .................................................... 18  
D. U of R ‘MyBackup’ Utility ................................................................................. 19  
  I. Installing ‘MyBackup’ program ......................................................................... 19  
  II. Creating a folder to store your backups ............................................................ 19  
  III. Clean out your My Documents folder .............................................................. 19  
  IV. Running ‘MyBackup’ for the First Time .......................................................... 20  

© 2010, University of Regina. All rights reserved.  
Revised – June 2012
Table of Contents

Chapter 5  NetStorage ................................................................................................. 23
A.  General Information on NetStorage ................................................................. 23
B.  Logging in to Netstorage ................................................................................. 23
C.  Downloading files from NetStorage ................................................................. 24
D.  Uploading files into NetStorage ....................................................................... 25

Chapter 6  Options for Backing up Data ................................................................. 27
A.  Information on External Backup Options ....................................................... 27
    I.  ReWritable CDs ......................................................................................... 27
    II. Portable USB drives .................................................................................. 27
B.  Backing up data to CD-RW .............................................................................. 28
    I.  Writing data to CD using Windows XP ..................................................... 28
C.  Backing up data to a USB Drive ....................................................................... 28
D.  Compressing Folders ....................................................................................... 29
    I.  Compressing Folders – “Zipping” ............................................................... 29
    II.  Decompressing Folders – “Unzipping” ...................................................... 30

Chapter 7  Cleaning Up Files and Folders ................................................................. 33
A.  Windows Disk Clean Up Utility ........................................................................ 33
B.  Unneeded Files and Folders ............................................................................ 33
C.  Clearing Recycle Bin ....................................................................................... 34

Chapter 8  Stay Secure on a Public PC ...................................................................... 35
A.  Public Terminals ............................................................................................... 35

Appendix A - Windows Backup Utility .................................................................. 37
A.  General Information on Windows Backup Utility ........................................ 37
B.  Backup using a Wizard .................................................................................... 37
C.  Setting a Backup to run Automatically .......................................................... 39
D.  Restoring files from Backup .......................................................................... 41

Appendix B - Windows File Management .............................................................. 45
A.  My Computer ................................................................................................... 45
    I.  Viewing the contents of a drive or folder ................................................ 45
    II. Selecting Files and Folders ....................................................................... 47
    III. Creating a New Folder ........................................................................... 47
    IV.  Copy ........................................................................................................ 47
    V.   Move ....................................................................................................... 48
    VI.  Deleting Files and Folders .................................................................... 48
    VII. Restore .................................................................................................. 49
    VIII. Renaming Files or Folders ................................................................... 49
    IX.  Undo Command ...................................................................................... 49
B.  Sharing Files .................................................................................................... 50
    I.  Creating a Shared Folder ........................................................................... 50
    II. Accessing Shared Folders on another system ......................................... 51
    III. Limitations on Folder Sharing .................................................................. 51
C.  Using Servers .................................................................................................. 51
D.  Saving a File ..................................................................................................... 51
    I.  Save As .................................................................................................... 51
    II. Save ......................................................................................................... 52
CHAPTER 1
VIRUS SAFETY

A. General Information on Computer Viruses

A computer virus is a computer program that is designed to replicate itself by copying itself into and infecting boot sectors, data files and programs stored in a computer. It may be benign or have a negative effect, such as causing a program to operate incorrectly or corrupting a computer's memory. Trojan Horses and Worms also fall in the category of Viruses. Trojan Horses often act as carriers for Viruses, and Worms can spread by themselves.

Once a computer has been infected with a virus, the first step is to run an anti-virus program to clean, or disinfect the machine. If the first option does not eliminate the virus then please call the IT Support Centre at 585-4685.

For more information on viruses go to the University of Regina website Computing Services>>Support>>Virus Info or http://www.uregina.ca/compserv/support/virusinfo.shtml.

Note: The first thing that should be done after the install of a new operating system on any computer is to install all Windows Updates and current Anti-Virus software.

B. SOPHOS Anti Virus - SAV

An anti-virus program is a software program designed to identify and prevent infection from known or potential computer viruses. At the University of Regina we support the virus program created by Sophos (SAV) for Windows. The University of Regina has licensed a number of Sophos antivirus products for use starting mid September of 2004. The University uses two Sophos products to provide virus protection to computers:

**Sophos Antivirus(SAV) and Sophos Remote Update** - The SAV product is used to detect and disinfect viruses on computer systems. The Sophos Remote Update program is used to check for updates to the Sophos Antivirus program and, when updates are available, download and install them.

All requests for support should be initially directed to the IT Support Centre at IT.Support@uregina.ca. If they cannot answer your SAV questions they will escalate the issue to the appropriate support staff. Users should not attempt to contact Sophos directly.

Note: The Sophos Antivirus software is for use only by University of Regina staff, faculty and active students. It is not to be installed or distributed by anyone not meeting these requirements.
C. **Using Sophos**

Computer viruses are often sent through email as an attached file. When the attached file is opened or executed, the virus is activated. Once a virus is active, your computer may become infected, causing problems with software.

As you use the GroupWise system on campus or any other email program worldwide you may receive emails with attachments. If the attachment is from an unknown source, the best option is to delete it immediately and eliminate the chance of infecting your computer with a computer virus.

Even if the attached file appears to come from a trusted source, there is still the possibility that the file will include a virus. Email addresses are sometimes forged. When in doubt, email the sender to confirm they are the true sender. If this is not possible, the attachment should be scanned for viruses before it is opened.

**To scan your Local hard drive:**

1. Open the email message.
2. Right-click the attached file.
3. Choose ‘Save…’
4. Select the folder location you wish to save it in, or choose Desktop. The CD drive is also an option.
5. If the file has a virus, SAV may detect the virus as soon as the file is saved.
6. If SAV does not open automatically, Go to Start menu, Programs, Sophos Anti-Virus.

7. Select ‘Set up a new scan’
8. Select the location of the scan – Example C: drive
9. The virus scan will take a few minutes and can be running in the background while you continue working.
10. SAV will inform you whether or not the file is infected with a virus. If in doubt, delete the file. Always err on the site of caution and contact the IT Support Centre for more information on how to proceed.
D. Updating SAV at Work, using Novell

Although SAV contains a comprehensive virus database, all users must regularly update these definition files. As new viruses emerge, new definition files are posted on the SAV website that will detect these new viruses. Keeping your SAV updated allows you the maximum protection against both old and new viruses downloaded from the Internet or hidden within an e-mail attachment.

To update SAV:

1. Log into Novell using your current username and password.
2. Any available updates to SAV will automatically be installed on your system.

Understanding SAV updates:

Sophos releases a new version of Sophos Antivirus monthly that includes the latest updates for detecting and removing all known viruses. In between each new version of SAV, Sophos released virus identity (IDE) files which contain detection and removal information for newly discovered virus.

For users on the campus network or who have high speed internet connections at home, the amount of data transferred on the monthly updates should be relatively painless. Users with 56K dial-up connections will have to endure a rather long download once a month, but for the remainder of the month updates should go very quickly.

E. Installing SAV at Home, or on campus without using Novell

Please see installation guide located at:
www.uregina.ca/compserv/support/sophos/index.shtml or follow the links
Computing Services>>Downloads>>Sophos – Download; Installation & Technical Notes

F. Updating SAV at Home, or on campus without using Novell

To Update SAV:

1. Sophos will update automatically each time you log onto your home computer and every hour thereafter.

Note: Users are especially at risk if they use Microsoft Outlook, Outlook Express, Eudora and other programs that automatically preview attachments before they can be scanned for viruses.
G. Email Virus Information

Computer viruses are often sent through email as an attached file. When the attached file is opened or executed, the virus is activated. Once a virus is active, your computer may become infected, causing problems with software or hardware.

As you use the GroupWise system on campus, or any other email program worldwide, you may receive emails with attachments. If the attachment is from an unknown source, the best option is to delete it immediately and eliminate the chance of infecting your computer with a computer virus. Even if the attached file appears to be from a trusted source, there is still the possibility that the file will include a virus.

On campus, emails are stripped of attachments with dangerous extensions as they are received into the email systems; however, virus checking is not inherent in GroupWise – which means that opening attachments off campus in Webmail on a PC without antivirus could lead to infection of that PC.

Note: If you receive an email from an unknown source, DELETE IT immediately. DO NOT OPEN an attachment from an unknown source.

Note: Many Email Viruses propagate by exploiting security holes in Windows – some of these holes have been repaired with Service Pack 2.
H. Disinfecting at Home

If you are running Windows XP at home and have become infected with a virus, you may notice that after each time you reboot you have to clean up that same virus. What has happened is that the virus has become part of the System Restore. To remove the virus from your System Restore, you can do the following:

1. Right click on the My Computer icon on your desktop.
2. Select Properties from the list
3. Select the tab called System Restore (you will not see this tab on your managed computer at work as you do not have access to this feature).
4. There is a tab marked 'System Restore',
5. Check the 'Turn off System Restore' option.
6. After turning off system restore, Windows will automatically delete the restore archives and any viruses that are contained within
7. The restore archives will also deleted.
8. You can then turn System Restore back on by un-checking the ‘Turn off System Restore’ feature.

Note: If you open My Computer on a managed system at work, you will notice that System Restore is not a tab option (as you do not have access to that feature at work).

I. Network Vulnerability

I. Shared Files and Folders

If you currently have shared folders on your computer, and are using an operating system other than Windows XP, you may be susceptible to viruses being placed on your machine through the use of a shared folder. To protect your machine, ensure that all shared folders are password protected, with a difficult password. Some viruses even include a list of commonly used passwords that the virus will use to attempt break in. Single user sign on will default to folders not being shared, reducing this risk.

Note: Shared folders on Windows XP machines are automatically password protected, and only users with a valid account on the machine are allowed to log in.

II. Open Ports

Many products that can be downloaded from the internet can make your system vulnerable to viruses and spyware. Examples of such products are ‘Kazaa’ (used for downloading music) and ‘WebShots’ (pictures that can be used as backgrounds and screensavers). These products, when installed, may create an open port on your machine that may allow viruses to be placed on your system and allow hackers into your machine through various methods. These ports will be open whenever your machine is connected to the internet. Open ports are also referred to as Backdoor Trojans.

III. Spyware

Spyware generally comes in the form of Data Miners used to collect data about you and what you are doing, then send it back to the hosting company. Most of the companies collecting this information sell your name and address info as part of an address list, but information such as banking numbers, passwords and IP addresses may also be collected and used by hackers.
Spyware is introduced to your computer in a number of ways including open ports; free downloadable games; and screen gimmicks such as Bonzi Buddies. As a general rule of thumb: if it can be downloaded free from the Internet, it will contain Spyware.

IV. Firewalls

On versions of Windows older than XP with Service Pack 2, it is a good idea to install a firewall, which assists with blocking unauthorized intrusions onto your computer. Zone Alarm is quite good and the home version is a free download.

With Service Pack 2 on Windows XP there is a built in firewall. For more information on Service Pack 2 see Computing Services Tech Note #1003 vo on the Computing Services website.

V. Spam

Spam is unsolicited commercial email, generally used to sell something. Spam can clog your inbox, waste valuable time and resources, and be offensive. There are a number of ways a person can prevent or reduce spam. For example: never make a purchase via spam or reply to spam; always use anti-spam software (most email service providers now provide spam filters with their service); delete messages without opening them; opt out of info offers on websites; and use blind carbon copy when sending/forwarding to a group of addresses.

VI. Hoaxes

Hoaxes are similar to spam, except they contain: warnings about viruses; requests for bank account info to get money safely out of some other country; and offers for free products, trips or money in exchange for forwarding to a certain number of addresses. These also clog email systems, promote harvesting of addresses for spam and in the case of virus warnings may cause companies to overreact. These messages should be deleted, and not forwarded on.

VII. Phishing

Phishing is the use of bogus emails and websites to trick you into supplying confidential or personal information. Typically you receive an email that appears to have come from a reputable organization, such as a bank. The “spoof” email contains what appears to be a link to the organization’s website, and requests personal information such as passwords, PINs and account numbers. If you follow the bogus link in the email it will lead you to a replica of the real site, where the hacker is collecting personal information.

These sites are often very well done, and look quite convincing. Never enter any confidential information with this type of solicitation. Legitimate companies will not send out these requests for confirmation of private info.
J. **Responsible Computing**

Having all of the latest security software installed still does not guarantee your computer will be safe. There are many little things that each of us do every day that leave our computer and data at risk.

Some simple things we can do personally to ensure our data remains safe:

1. Shred all confidential papers that are no longer required.
2. Do not leave notes lying around with user IDs and passwords written on them.
3. Shut down your computer when you are going to be away from it for an extended period of time.
4. Do not leave applications open and signed on when you leave for the night.
5. **Lock your workstation whenever you leave your desk.**
6. Be aware of the website you are on - is it secure https:// or non-secure http://
7. Erase data from old CD’s and disks, then damage them before disposing.
8. Wipe old hard disks with a certified wipe program.
9. Change passwords regularly to difficult words or letter/number combinations.
10. Be aware that most data can be recovered on a hard drive or removable medium; even it if it has been deleted. This recovery process is very expensive, but ensure you are not disposing of things that would make it a worthwhile expenditure for a data thief.
11. Be kind to other online users at work and do not listen to online radio – the bandwidth required for this is adds up quickly, and affects everyone’s response.
12. Be aware that any correspondence conducted over tools such as MSN are routed through a server in the US, and as such are subject to US not Canadian privacy laws.
A. **Windows Updates**

Microsoft has recently issued a number of new security updates for Windows XP computers. These have been grouped together into a package called Service Pack 2. It is important that you install this update at home. This can be done using the following method to obtain Windows Update patches. Included in these updates are a built-in firewall and increased security from viruses and worms. These updates are completed automatically when University of Regina users log in to Novell.

**To install Windows updates on your system:**

1. Start Internet Explorer
2. From the ‘Tools’ menu choose ‘Window Update’
3. Choose ‘Install’
4. You must have administrator rights to your workstation to complete this procedure.

**Note:** For more information on Service Pack 2 see the University of Regina website under Computing Services>>Support>>Technical Notes>>#1003 or http://www.uregina.ca/compserv/support/technotes/1003/cctn1003.shtml

**To set your computer to run the Windows update automatically:**

If you are running Windows XP it is possible to set the Windows update to run automatically in the back ground while you are on the internet. This is the recommended method so your PC always has the most current operating system possible.

1. Start Internet Explorer
2. From the ‘Tools’ menu choose ‘Internet Options’
3. Choose the ‘Advanced’ tab in the Internet Options box
4. Check off ‘Automatically check for Internet Explorer updates’
5. Close Internet Options window

B. **Cookies**

When you visit a website, it may place a small data packet called a ‘cookie’ on your computer. This enables the site to remember your details and keep track of your visit. Cookies do not pose a threat to your data; however, they do threaten your confidentiality. If you prefer to remain anonymous, use the security settings in your browser to disable cookies. If you disallow cookies there may be some sites you are unable to view, or some customizable features you are unable to take advantage of.

There are two types of cookies: First Party which are from the originating site; and Third Party or Foreign cookies which are from some third party site, collecting data through the originating site.
To change settings in Explorer:
1. On the Tools menu, click Internet Options
2. Choose the Privacy tab
3. Use the sliding bar to choose the level of security you would like
4. As you move the sliding bar, there will be a description of the level that level of security.

Note: Default setting is Medium. Recommended setting is Medium, or Medium-High.

To change settings in FireFox:
1. On the Tools Menu, select Options
2. Choose the Privacy icon
3. In the Cookies area, select the setting you would prefer and check/uncheck the save cookies option.

Note: Default setting is ‘Enable all Cookies’ Recommended setting is ‘Enable cookies from originating website only’.

C. Saving Internet Passwords

More recent versions of Windows Explorer and Netscape Navigator can remember user IDs and passwords, which can have a negative impact on security. Setting your browser to AutoComplete passwords means that all of your IDs and passwords are stored on your computer, increasing your vulnerability.

Although these passwords are encrypted, there has been growing concern about the ability to break the encryption algorithm. If you set AutoComplete on when using any public computer (such as in a public lab), it enables other people to log onto your accounts.

To disable AutoComplete in Internet Explorer:
1. Open Internet Explorer, select Tools, Internet Options
2. Click the Content tab
3. Under Personal information, click AutoComplete

4. Deselect the check boxes for the AutoComplete options.
5. Press the 'OK' button

To adjust Password Manager in Firefox:

1. Open Firefox, Tools, Options
2. Choose the Privacy option on the left.
3. Click on Saved Passwords.
4. Deselect the Remember Passwords checkbox
5. Press View Saved Passwords button
6. From here you can delete any previously saved passwords on the computer.
D. **Popup Blockers**

Pop ups can be annoying, and can also compromise the security of your PC. Windows XP has included a popup blocker as part of Service Pack 2. To enable or disable go to Windows/Tools/Pop-up Blocker. The first option on this menu is to enable or disable. The second option Pop-up Blocker Settings, allows you to set the level of security, as well as specify sites that should never be blocked.

E. **Temporary Internet Files**

While browsing (using Internet Explorer), your browser saves files from the pages you visit to the “Temporary Internet Files” folder. The idea is that when you browse at a later time the computer will search this folder first to see if any of the pages are already saved in order to save time. This speed decreases as the folder becomes cluttered with more and more files, so it becomes necessary to clear this folder from time to time.

To clear the “Temporary Internet Files” folder:

1. Open Internet Explorer, Tools, Internet Options
2. In the middle pane click on Delete Cookies and Delete Files (the latter may take a while) and then select OK.

Note: This should be done at startup or just before shutdown to avoid any complications. It should also be done on a regular basis.

F. **Cache Clearing**

Another consideration for keeping your computer clean and safe is cache clearing. While surfing the internet, an extensive history is recorded in your cache. This can create a security risk if you are using a public computer.

To set your cache to clear by default on exit from Internet Explorer:

1. Open Internet Explorer, Tools, Internet Options
2. Select the Advanced Tab
4. Check off Empty Temporary Internet Files folder when browser is closed.
5. Select the OK button

To clear the cache manually upon exit from Internet Explorer:
1. In Internet Explorer, on the Tools menu, click Internet Options.
2. Select the General Tab

3. Within the Browsing history area, select Delete beside Delete temporary files, history, cookies, saved passwords, and web form information.
CHAPTER 3
PASSWORD SAFETY

A. General Information on Passwords

At the University of Regina, you may have several passwords such as Novell, Banner, and UR self-service. They MUST all be changed the first time you login and periodically thereafter.

B. Changing your Passwords

To change your password for Banner:
1. Log into Banner using your current username and password
2. In the Direct Access box type GUAPS WD and press enter
3. Enter your current password
4. Enter a new password
5. Enter the new password again to verify
6. Click the Save button or press F10

Note: Password must be at least 6 letters and 1 digit.

To change ur egina.ca password (Novell, GroupWise, URPPP and UR Courses):
1. Open Netscape or Internet Explorer
2. Go to the IT Support Centre webpage at http://www.uregina.ca/compserv/ ITSC
3. Click ‘Staff and Faculty Information’
4. Click ‘Change Passwords Form’
5. Select the link titled ur egina.ca password webpage
6. Enter your Username and Current Password
7. Enter a New Password
8. Enter the New Password again to Verify
9. Click the ‘Change Password’ button

To change UR self-service PIN (FAST, Web Mark Entry, Web for Employees):
1. Go to the Main U of R Homepage: www.uregina.ca
2. Navigate to ‘Faculty & Staff’>>UR Self Service Login
3. Log into Banner Self Service using your current 9-digit ID and 6-digit PIN
4. Choose Personal Information
5. Choose Change PIN
6. Enter your old PIN
7. Enter a new PIN twice
8. Click the Change PIN button

To change your password for detailsOnline (MasterCard purchasing card):
1. Log into detailsOnline at www.bmodetailsonline.com
2. Select Change Your Password from the Quick Link drop down menu located on the home page
3. Click Go.
4. Enter current password
Enter new password and verify.

6. Complete the password reset section to receive a temporary password if needed in the future.

7. Select Save Changes from the side menu.

**Strong Password Characteristics**
- Are at least eight alphanumeric characters long.
- Have digits and punctuation characters as well as letters (Note: Oracle allows only the special character underscore (_) in a password, unless the password is enclosed in quotes.)
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

**Weak Password Characteristics**
- The password is the same as your user name or login name.
- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as names of family, pets, friends, computer terms, birthdays or other personal information, or number patterns like aaabbb, dddddd, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

**A List of Don’ts**
- Don't reveal a password over the phone or in person to anyone. Not your boss. Not your family. Not your co-workers. If someone demands a password, refer them to this document.
- Don't reveal a password in an email message.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Passwords should never be written down or stored unencrypted on-line.
- Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, MSN).
- Don't use the default password, if one is provided. Change it immediately to a new, stronger password.
CHAPTER 4
NETWORK DRIVES

A. General Information on Network Drives

The Network Drives are other areas that your computer is connected to that are physically located on other computer systems on the University of Regina network. The University of Regina has a server system in which every employee, faculty member and staff have space in which they can place files and folders where they will be backed up every night.

You may have access to some network drives, depending on the setup of your Novell account. Information stored on network drives is shared only with users that have permission to access certain folders on the network drives.

I. Benefits of using a network drive

a) All data is backed up every night, so even if you have a hard drive problem with your computer your files are still safe and recoverable.

b) Files stored on a network drive are accessible to you from the internet wherever you are, by using NetStorage and your Novell login.

II. Network Drives at the University of Regina

a) The I:\ Drive is your personal storage space on the Network.

b) The T:\ Drive provides storage and secure access to folders for use by departments as requested.

c) The S:\ Drive houses the Banner forms and Banner related information.

d) Some departments may have access to other drives such as L:\, M:\, or P:\ which provides secure access and storage similar to the T:\ drive.

e) Some faculties provide a 2nd home directory called the H:\ drive. If not, the H:\ is the same as the I:\ personal drive.

III. Files and Folders on Local Disk (C:)

Local Disk C:\ is reserved for Program files and required software. You should not save files in the C: folder. In the event that there is a problem with the system, Local Disk C:\ would be re-installed and information you saved on the C: drive would be lost.
IV. Files and Folders on Local Disk (D:)
Local Disk D: is available for you to create folders, save files, install software and manage files. In the event that there is a problem with the system, and Local Disk C: is re-installed, the information you save on the D: drive would be saved and reloaded for you. The user information stored on C: through your Novell login and use of the My Documents folder on the desktop will also be saved and reloaded if possible.

B. Access to Network Drives

I. I: drive
The I: drive provides storage for your files that only you can access. There is an initial maximum allotment of 300mb. If 300mb is not enough storage for your important data, please review the options provided in Chapter 5 – Options for Backing up Data.

II. T: drive
There is space available on the Network Drive T: for departments who share a lot of data, but will no longer be able to do so effectively with Windows XP. For information that used to be stored in a shared folder on one machine, there is now the option to store this information on the T: Drive, and give access only to those that require it. For more information, or to request space on the T: Drive for your area, please contact the IT Support Centre at 585-4685 or IT.Support@uregina.ca.

C. Saving Files to a Network Drive

Files can be manually copied or saved to the I: drive, or automatically updated using the University of Regina ‘My Backup’ utility.

I. Copying existing files to a Network Drive
   a) Select the files and/or folders you would like to back up
   b) Copy the files and/or folders
   c) Navigate to the I: Drive using the ‘My Computer’ icon, or the ‘Windows Explorer’ icon.
   d) Paste the files to the I: Drive

II. Saving new files directly to a Network Drive
   a) Choose File, Save As
   b) In the File Name box, type a name
   c) Select the appropriate drive letter and folder name
   d) Choose Save

Note: For information on managing files and folders see Appendix A.
D. **U of R ‘MyBackup’ Utility**

The University of Regina has a backup program created specifically for backing up files to a network drive. This program will automatically back up any changes to existing files, and backup any new files that are created and saved in your ‘My Documents’ folder, or other folder(s) you select.

I. **Installing ‘MyBackup’ program**

To install ‘MyBackup’ software:

1. Navigate to the S:\ drive using My Computer or Windows Explorer
2. Double-Click the ‘Dist’ folder
3. Double-Click the ‘win32’ folder
4. Double-Click the ‘mybackup’ folder
5. Double-Click the file ‘Setup.exe’

OR

1. Click ‘Start’, then ‘Run’
2. Type in the following path: \S\dist\win32\mybackup\setup.exe
3. Click OK to begin the Install process.

Note: Accept the default values presented by the installer by clicking OK when prompted. *MyBackup* will be added to the ‘StartUp’ program group, so that *MyBackup* will run every time your PC is booted.

II. **Creating a folder to store your backups**

To create a Folder on your I:\ drive:

1. Open My Computer or Windows Explorer
2. Locate your I:\ drive and double-click on it to open it
3. Click ‘File’ on the top menu bar
4. Choose ‘New’, then choose ‘Folder’
5. Type a name for your new folder, such as ‘MyBackup’
6. Press Enter

III. **Clean out your My Documents folder**

1. Move all personal files to the D:\ drive or somewhere that will not be included in the regular backup.
2. Clean up business files, so only those truly requiring backup will be included.
IV. Running ‘MyBackup’ for the First Time

The first time you run MyBackup, you tell the program where to find the files that are to be backed up, where to put them, and how often to do the backup. MyBackup will then proceed to copy all the files. It will then ‘go to sleep’ until the next scheduled interval, at which time it will copy any files that are new or changed since the last backup.

Note: The first reboot after MyBackup has been installed will add it to your System Tray.

To Configure MyBackup:
1. Click on Start
2. Point to All Programs, then Startup, then ‘MyBackup’
3. Click ‘Configure’ to open the Configuration window
4. Click the upper ‘Select’ button to set the folder to copy files from
5. Choose the Drive you wish to backup FROM and Click OK.
6. Choose the Folder you wish to backup FROM and Click OK.
7. Click the lower ‘Select’ button to set the folder where the backup files will be stored
8. Choose the Drive you wish to backup TO and Click OK
9. Choose the Folder you wish to backup TO and Click OK
10. Enter the interval, in minutes, you want to have between backups.
11. Click OK.
12. The main ‘MyBackup’ window will display the message ‘Backup in Progress’, and all files, and subfolders within the selected folder, will be backed up.
13. Once the first backup is complete, the MyBackup window will tell you when the next backup will occur.

14. Click the minimize button \( \text{\textbullet} \) to move the Backup message to your task bar.
15. Do not close the program using the \( \text{\texttimes} \), unless you want to stop the backups from running.

**Note:** If you remove a file from a backed up folder on your hard drive, the corresponding backup copy will be kept for 7 days and then deleted.

**Note:** Do NOT erase your backup files. MyBackup will not recopy files; it only copies new or changed files. If you want a complete new backup, first delete the existing backup folder to save space, then create a new folder on your backup disk and tell MyBackup to use the new folder.
CHAPTER 5
NETSTORAGE

A. General Information on NetStorage

The NetStorage system allows an interface between you and your network file storage from a web browser no matter where you are located, without the installation of any software.

The web address to access Net Storage is: https://netstorage.cc.uregina.ca/

Within the Netstorage system there are some known issues. If you are logged into Novell and have the file open then the file cannot be accessed from NetStorage because it is locked. The only solution is to remember to close the file at work before leaving if you are expecting to want to access it from home using NetStorage. Also, occasionally right clicking on a file and choosing download doesn’t work. You can still download the file by double clicking on it.

Note: To access Netstorage you must use Internet Explorer or Netscape version 6.2 or greater.

B. Logging in to Netstorage

1. Navigate to the NetStorage website: http://netstorage.cc.uregina.ca
2. Click the Access NetStorage Link. OR
3. Go to the U of R website >> Quicklinks >> Computing Services >> Net Storage (under News, Announcements & Current Events)

The Netstorage interface allows you to: software.

Access NetStorage

4. You will be prompted to Log in to the NetStorage system. The User name is your Novell Login ID and the password is your Novell Password.
5. Once logged in you will have access to the various drives you normally see at work using ‘My Computer’ or ‘Windows Explorer’

Note: The Home@UOFR drive represents your personal I:\ drive.
C. Downloading files from NetStorage

To Download a file from NetStorage:
1. On the left hand side, click the drive you wish to view.
2. The folders and files will be shown in the main frame.
3. Navigate to the appropriate folder on the left.
4. Select the file you wish to download in the main frame.

Note: You may not be able to see all the files in the folders. It will only show the first 25 files, listed in alphabetical order. To see the next 25 files you must use the scrollbar at the bottom.

5. On the NetStorage menu, click File - Download.

6. An option box will pop up, asking if you want to open or save the file.
7. Click Save.
8. Select the location/folder where you wish to save the file on your hard drive.
9. Click Save.
10. The file will be saved in the location you selected.
D. Uploading files into NetStorage

To Upload a file into NetStorage:

1. On the left hand side, navigate to the drive and folder that you wish to upload a file into.
2. On the NetStorage Menu, click File – Upload
3. Click Browse
4. Locate the file you wish to upload and click Open
5. Click Upload
6. The file will be uploaded from your hard drive to the Network drive
CHAPTER 6
OPTIONS FOR BACKING UP DATA

A. Information on External Backup Options

There are a number of ways that data can be backed up external to your PC and the network. The two most popular and convenient are Writeable CD’s and USB drives.

I. ReWritable CDs

A CD-ReWritable (CD-RW) drive is a good way to back up data. CD-Recordable (CD-R) media and CD-ReWritable (CD-RW) media can store 700 – 800 MB of data each, and the files are easily accessible by inserting the disc into any CD-Rom or CD-RW drive.

CD-R means you can only record data. You cannot save overtop of other data, and once the disc is full it can only be used to retrieve data. CD-RW means you can re-write to the disc. If the disc is full you can choose to store data that replaces data that was already on the CD. The CD-R media is less expensive, and is fine for archiving data. The CD-RW media is more costly, but can be used more than once.

A CD-RW drive is standard on all Evergreen machine dated 2004 and newer. The LG drive can playback a standard CD at 52 speed, record to a CD-RW at 24 speed, and record to a CD-R at 52 speed.

Note: There are several other makes and models of CD-ReWritable drives. The LG brand is currently supported by Computing Services, but you may find other drives that suit your needs as well.

II. Portable USB drives

There are a number of names for these portable drives including USB Memory, Flash drive, Stick drive. These drives are used by simply plugging them into a USB port. They have a wide range of capacity from 128 MB to several GIG, and it is possible to buy portable drives that are password protected for sensitive data. The advantage of a portable drive is their versatility, it is not necessary to have a burner or burner software to use a portable drive and the space can be reused just like the hard drive on you PC.

On the new Evergreen machines, there is a USB port of the front of the tower, making access to the data on these drives very easy. Older models usually have a USB drive, but it may be on the back of the tower.
B. Backing up data to CD-RW

Windows XP has built-in capability to record data to a CD-RW, or you can use the software provided with the LG CD-RW drive.

I. Writing data to CD using Windows XP

1. Open ‘My Computer’ by double-clicking the icon on your desktop
2. Navigate to the folder where the files you wish to save to CD are located
3. Open the folder
4. Select the files by holding down the CTRL key as you click the files you want
5. Click Edit-Copy
6. Navigate to your CD-RW drive (usually Drive E:\ on a University Evergreen system)
7. Double-click the drive to open it
8. Create a new folder on the CD, if you wish:
   a) Click File- New- Folder
   b) Type a name for the new folder
   c) Press Enter
   d) Double-Click to open the new folder
9. Click Edit-Paste, to copy the files you selected to the E:\ drive
10. Insert a CD-R or CD-RW disc in to the E:\ drive
11. Click ‘Write these files to CD’ on the upper left side of the screen

Note: Be sure to close the program you are using before removing the portable drive, this will ensure that all the program has completed writing data to the drive and prevent damage to it.

C. Backing up data to a USB Drive

1. Plug the portable drive into a USB port
2. A new drive will appear on the list in My Computer or Windows Explorer
3. Copy, paste or save data to this drive just as you would to your hard drive
4. Wait until the data has all been written to the drive before removing it
D. Compressing Folders

Windows XP has an existing compression program when it is installed on your PC. If you are running Windows 98 you will need to download a program to do this for you: “WinZip” is the standard program.

You can use these programs to shrink the size of any of your folders. The amount of size saved will differ greatly depending on the type of files in the folder.

I. Compressing Folders – “Zipping”

1. Highlight the folder you wish to compress. Select File, Send to, Compressed (zipped) folder.

OR

2. Right click on the folder and select Send to, Compressed (zipped) folder.
3. A second folder will appear, with a zipper on the icon, and a .zip extension.
4. If you check the properties of the two folders, you will see that the file size is reduced.
II. Decompressing Folders – “Unzipping”

1. Select the zipped folder and select File, Extract all. Or right click on it and select Extract all.

3. The wizard will appear to guide you through the process.
4. Click Next.

5. Select a location to extract to by clicking Browse.
6. Click Next.
7. Click Finish.
Cleaning files from your computer is a very important and useful activity. This will keep your computer from using up unnecessary memory storing old temporary files. You’re my document’s folder is one location where old files may accumulate and use up unnecessary hard drive space, and your I: drive is another location. Checking these locations from time to time to make sure the files are current is a quick space saving technique.

Note: Disk clean up will remove all temporary files from your machine

A. Windows Disk Clean Up Utility

To perform a disk clean up:

1. Click Start, Programs, Accessories, System Tools, Disk Clean Up
2. Select the drive you would like to clean up
3. A list of files to be removed will be displayed

![Disk Cleanup window]

4. At this point you can review the files if there is any need too
5. Click OK
6. Click OK

B. Unneeded Files and Folders

You should periodically check your ‘My Documents’ folder, I: drive and any other drive folders you have access to, and ensure there is no unnecessary duplicates or old unneeded files being stored on your machine or on the network servers.
Be careful that you do not delete files from the *MyBackup*, folder. *MyBackup* will not recreate deleted files, it will only update files that indicate a change since the last backup.

Note: For information on managing files and folders see Appendix B.

C. Clearing Recycle Bin

It is also a good idea to periodically clear out the recycle bin on your hard drive. The recycle bin contains all of the files that you have deleted recently off of you hard drive. The reason files are moved into the recycle bin is to allow you to restore them if they have been deleted in error. This is a handy feature, but can also cause a backlog of old files on your computer if they are not cleaned up periodically.

To empty the Recycle Bin:

1. Double click on the Recycle Bin icon on your desktop.
2. Select File
3. Select Empty Recycle Bin
4. Click Yes for Confirm Multiple File Delete.
A. Public Terminals

A few quick clicks and keystrokes will keep you safe when using a public terminal.

by Neil J. Rubenking

1. Before you start, turn off dangerous browser settings. In Internet Explorer’s Options dialog click the Content tab, click the Settings button in the AutoComplete pane and uncheck all the boxes. In Firefox’s Options dialog click the Privacy tab and uncheck all the boxes under History and Cookies, then click the Security tab and uncheck all the boxes under Passwords.

2. Be careful not to visit any financial Web sites by clicking hyperlinks received in your Web-based e-mail. The sites they bring you to might be fraudulent, and the public computer may not have antiphishing software enabled. If you need to visit a bank or other financial Web site, type the URL yourself.

3. Before entering any sensitive data on the public computer, keep in mind that no software will detect a hardware keylogger, so limit your sensitive transactions to those that are utterly essential.

4. When you’re finished with the browser, erase your tracks. In Firefox press Ctrl-Shift-Del and check all the boxes, then click OK. In IE select Delete Browsing History from the Tools menu and click Delete all.

5. When you are all done, launch My Computer, right-click the icon for the hard disk, and click Properties. Click the Disk Cleanup button and wait for the list of choices. Make sure that Recycle Bin and Temporary files are checked and that Compress old files is not checked. Then click OK to clean up.
APPENDIX A
WINDOWS BACKUP UTILITY

A. General Information on Windows Backup Utility

The Windows Backup utility takes the files from a folder you select (usually your ‘My Documents’ folder) and creates a backup file on a network drive (usually your personal I: drive). The Backup utility creates a file with a .bkf extension. There is an option to set the backup to run automatically.

Note: The Backup utility does NOT store your files individually, and therefore files backed up using this utility will NOT be accessible to you via NetStorage. If you have files you need to access through NetStorage, use the methods listed in Chapter 3 – Section C - Saving Files to a Network Drive

B. Backup using a Wizard

To backup your files to the I: drive using the wizard:
1. Click Start, Programs, Accessories, System Tools, Backup
2. A wizard will start taking you through all the steps required in running a backup
3. Click Next
3. Choose ‘Back up files and settings’
4. Click Next

5. Select what you want to back up and Click Next
6. Once you have reached the following screen you will need to click the browse button to navigate to the I: drive

7. Click Next
8. Click Finish
9. A pop up window will provide a summary of the backup information
Click Close

C. **Setting a Backup to run Automatically**

To backup your files to the I: drive automatically:

1. Follow the same steps as shown in Section B, as if you were running a normal backup. When you get to step 8, click the ‘Advanced’ button instead of the ‘Finish’ button.

2. Leave the backup type at normal and click next

3. Select any options you may wish

4. When you reach the following screen click the later option
5. Enter a Job Name
6. Click the ‘Set Schedule’ button
7. Choose from the various options to select the frequency of the backup

8. Click OK
9. You will be prompted to enter a password, enter your Novell password and choose OK. If you change your Novell password you will be have to change your ‘my Backup’ password separately
10. Click OK and the backup will begin
11. Once it has completed you will see the following window

12. Click OK to continue
D. Restoring files from Backup

If a file on your hard drive becomes corrupt or is lost, if you want to revert back to the version of a file that was backed up, or if you want to restore files that have been deleted, you can restore the file from the backup.

To Restore a file from backup
1. Navigate to your I:\ drive
2. Double-click the ‘.bkf’ file
3. The Backup or Restore Wizard will start
4. Click Next.
5. Click the button next to ‘Restore files and settings’
6. Click Next
7. A window will pop up, showing the available .bkf files you can choose to restore from.
8. Double-click the .bkf file you want to restore files from.
9. Expand the folders that are underneath, and select the files you want on the right hand side by turning the on or off . Only files with the checkmark on will be restored.

10. Click Next

11. To continue with the restore as shown, click Finish
| Note:        | If you want the files to be restored to somewhere other than the ‘original location’ OR if you want the existing files to be replaced with the older backed version, click the Advanced… button to change the settings. |
A. My Computer

My Computer and Windows Explorer are the main tools for viewing and managing the files and folders on your hard drive, floppy drive, or any other storage medium. These tools allow you to do everything from copying a file to another folder to launching an application to examining how much space is available on your hard drive.

I. Viewing the contents of a drive or folder

To view the contents of a drive or folder:
1. Double click on the drive or folder you wish to view.
2. Another window will open displaying the contents.

To use only one window:
Having many screen open at once can some times ‘clutter’ the screen, therefore, you may change this setting so that My Computer only uses one window to display information.

1. Choose Tools, Folder Options.
2. Under the General Tab, under Browse folders, click the button ‘Open each folder in the same window’.
3. Choose the OK button.
4. Choose the Close button.

To view file extensions:
1. Choose Tools, Folder Options.
2. Click the View tab at the top.
3. Turn off the check mark that appears in front of Hide File Extensions for Known File Types by clicking on it.
4. Click the OK button.

Note: You can apply your selected settings to all folders by clicking the ‘Apply to All Folders’ button.
II. Selecting Files and Folders

Before any action can be taken on an object such as a file or a folder, it must first be selected. Once an object is selected, you can then move or rename or copy the object.

To select a single file or folder:
1. Click once on the file or folder.
2. When the file/folder is selected it will appear in reverse color.

To select a continuous group of files or folders:
1. Click on the first file that you wish to select.
2. Hold down the SHIFT key and click on the last file you want to select.

Note: An alternative method for selecting a group of files that are next to each other is to hold down the mouse button and drag a rectangle around the files you want to select. You must start to do this in a white area of the screen.

To select a non-continuous group of files or folders:
1. Click on the first file you wish to select.
2. Hold down the CTRL key and click any other files you want to select.

To select all the files and folders in the window:
1. Choose Edit from the menu.
2. Then choose Select All.

III. Creating a New Folder

Folders are used to organize your information in a manageable way. Folders can contain subfolders, shortcuts and/or files. They can be placed on your desktop for easy access or left in your hard drive.

To create a folder:
1. Open the folder in which you want to create a new folder.
2. Choose File from the menu.
3. Choose New, Folder.
4. A new folder is now visible on the screen with the title New Folder selected. Simply type a name for the new folder over top of the temporary name.
5. Press Enter.

IV. Copy

Good file management involves knowing how and when to move, copy delete, and rename files and folders. We’ll start with copying files and folders. There are at least three different methods for copying files or folders. You can adopt one method and use it all the time, or you can pick and choose from the various methods. Whatever works for you is the best way. Remember that when you copy a file or folder the original remains where it was a duplicate is created (and perhaps place in a new location).

To copy a file or folder:
1. Locate the file or folder you wish to copy.
2. Select the file or folder by clicking once on it.
3. Copy the information using one of the following methods:
   a) Choose Edit, Copy from the menu,
   b) Click the Copy button from the toolbar,
   c) Click with the Right Mouse Button on the file and then select Copy from the shortcut menu.
4. Locate the destination folder and open it.
5. Paste the file or folder using one of the following methods:
   a) Choose Edit, Paste from the menu,
   b) Pick the Paste button from the toolbar,
   c) Click with the Right Mouse Button on the window where the copy is being located and then select Paste from the shortcut menu.

V. Move

Remember that when you move a file or folder, it is no longer in the original place it was created.

To move a file or folder:

1. Locate the file or folder you wish to move.
2. Select the file or folder by clicking once on it.
3. Cut the information using one of the following methods:
   a) Choose Edit, Cut from the menu,
   b) Click the Cut button from the toolbar,
   c) Click with the Right Mouse Button on the file and then select Cut from the shortcut menu.
4. Locate the destination folder and open it.
5. Paste the file or folder using one of the following methods:
   a) Choose Edit, Paste from the menu,
   b) Pick the Paste button from the toolbar,
   c) Click with the Right Mouse Button on the window where the copy is being located and then select Paste from the shortcut menu.

VI. Deleting Files and Folders

When you delete a file or folder the Recycle Bin protects the user from over-hasty deletions because the deleted file or folder is not instantly deleted but can be retrieved from the Recycle Bin if you later decide you want it back.

To delete a file or folder:

1. Locate the file or folder you want to delete.
2. Select the file or folder by clicking once on it.
3. Delete the information using one of the following methods:
   a) Click on the Delete button from the toolbar,
   b) Click with the Right Mouse Button on the file or folder and select Delete from the shortcut menu.
   c) Click the Delete button on the toolbar.
4. Click the Yes button to complete the process.

Note: You can also drag file or folder icons onto the Recycle Bin icon.

Note: If you delete a file at the DOS command prompt or from a floppy disk, it does not go into the Recycle Bin. Also, if you hold down Shift while deleting a file, it will not go into the Recycle Bin. Be careful, as files cannot be restored if you bypass the Recycle Bin.

VII. Restore

If you inadvertently deleted vital documents and want to restore them you must get them from the Recycle Bin.

To restore a file or folder:
1. Double Click on the Recycle Bin.
2. Select the file(s)/folder(s) you want restored.
3. Restore the file(s) using one of the following methods:
   a) Choose File, Restore,
   b) Click on the file(s)/folder(s) with the RIGHT mouse key and then pick Restore.

VIII. Renaming Files or Folders

Occasionally you will need to rename a file or folder. If you rename a file be sure that you include the original extension name (such as .doc or .xls) in the new name otherwise Windows may not know what type of file it is and may not be able to create any type of association.

To rename a file or folder:
1. Select the file or folder you wish to rename by click once on it.
2. Rename the file or folder using one of the following:
   a) Click a second time on the name of the file or folder
   b) Right click on the file or folder and select Rename form the popup menu.
3. Type the new name for the file or folder.
4. Press Enter.

IX. Undo Command

When you move, copy or rename something, the command to undo that action is remembered by Windows. And Windows remembers the last action you performed first, the next to last second, and so forth. The most important thing about Undo is to use it as
soon as you realize you’ve made an error. You don’t want to continue working and then use Undo because you will undo what you’ve just done and not what you want to undo. So if you do make a mistake, stop and use Undo right away to set things straight.

To undo an action:
1. Use one of the following to undo:
   a) Click the Undo button on the toolbar,
   b) Right click in a free area of the folder and choose Undo,
   c) Choose Edit, Undo from the menu.

B. Sharing Files

I. Creating a Shared Folder

To make a folder shared:
1. Open either ‘My Computer’ or ‘Windows Explorer’
2. Navigate to the Folder you wish to share
3. Click the Folder, but do not open it
4. Click the Share this Folder link
   OR
   Click File on the Menu bar, then Click Sharing and Security…
5. The share properties window will pop up
6. Click the ‘Share this folder’ radio button
7. Click OK.

Note: You can only share a folder or file with another user on the network who has an account on your machine.

To create an account on your machine:
Each user that will require access to shared files or folders on your machine must log in to your machine using their Novell username and password. This will create an account for them, and allow them to access your shared files and folders.
II. Accessing Shared Folders on another system

To access shared files on a system running Windows XP Professional, the user trying to get the files must have their own user account on that machine.

To create a user account, the user must log into Novell on the machine where the files are shared. Once this account is created, they can then access shared files and folders for their own system.

III. Limitations on Folder Sharing

Windows XP limits the number of users connecting to a system. Only 10 users may connect at one time. Any user that is connected for more than 15 minutes without any activity will be logged out automatically.

C. Using Servers

There is space available on the Network Drive T: for departments that share a lot of data, but will no longer be able to do so effectively with Windows XP. For information that used to be stored in a shared folder on one machine, there is now the option to store this information on the T: Drive, and give access only to those that require it. A major benefit of using the T: Drive is that the files are backed up every night. For more information, or to request space on the T: Drive for your area, please contact the HelpDesk by emailing HelpDesk@uregina.ca or phone 585-4685.

D. Saving A File

The text you type into a new document and the changes you make to an existing document are held temporarily in the computer's memory. To retain this information, you must save the document to a disk (the hard disk, floppy disk, or a server disk).

I. Save As

When you save a file for the first time it must be given a name. Filenames consist of two parts, the first part is the filename and the second part is the extension. The filename may be from 1 to 256 characters in length. The extension may be 1 to 3 characters but the extension is typically added automatically by the MS programs. In Word the program will automatically attach DOC as the extension. There are certain characters that are invalid when naming files (*, >, <, ?, to name a few).

To save a new, unnamed document:
1. Choose File, Save As.
2. In the File Name box, type a name.
3. At this point you may also choose a different drive and/or folder.
4. Choose Save.

II. Save

After adding text to a document you need to resave the file with the changes. You should make a practice of saving quite frequently. This command will save the new information and leave the file on the screen so you may continue to work in it.

To save an existing document:

1. Choose File, Save OR click the Save button.

Word saves the document with its current name. If you haven't given the document a name, Word displays the File Save As dialog box.