SECURITY & WELL-BEING

Protecting Data

Data security – is concerned with protecting software and data from unauthorised tampering or damage. IT departments often attach more importance to data protection rather than hardware protection. Recovery of lost data is often more expensive than replacing damaged hardware.
Sensitive data should be safeguarded against unauthorised access. In a network environment, the system administrator provides a unique user ID and a password to each computer user. The user ID and password are needed to logon to the networked computer.
Home users are able to set up a start-up password through their operating system. You should also set a password to unlock your screen saver. You can also set password protection to data files.
The use of a strong password enhances the security of your computer system. Your password should be at least 6 characters long. It should consist of both upper- and lower-case letters and also one or more numbers. Your date of birth, phone number or any word that can be found in a dictionary do not constitute a strong password. Passwords should be changed regularly.
Never share or disclose your password to any other person including colleagues, family members etc. Do change your password if you suspect that somebody knows it.

Firewall

A **firewall** is a system designed to prevent unauthorised access to your computer system when connected to Internet. A firewall is simply a program or hardware device that filters information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. Many users having always-on connections (such as ADSL or cable) are encouraged to install personal firewalls (software) that protects their system from intruders.

Updating Software

We strongly recommend that you turn on Windows automatic updating so that Windows can install security and other important or recommended updates for your computer as they become available.
Computer programs such as operating systems, email clients, browsers, media players and desktop applications (e.g. wordprocessors, spreadsheets, databases etc.) may have vulnerable defects through which intruders can gain access to your computer. Software vendors usually release patches or hotfixes for their products when a security vulnerability is discovered. You must ensure that all programs on your computer are updated with the latest available patches. You should also check for any available updates when installing new software.
Software patches can often be downloaded for free from the vendor's website. Some programs (e.g. MS Windows) have utilities which automatically connect to the vendor's website and download any available patches. If there is no automatic update feature for any of your programs, visit the vendors' website regularly and download any available updates.

Malware

Malware (malicious software) is a program designed to secretly enter and damage a computer system. Malware includes:

- A computer virus is a piece of program designed and written to make additional copies of itself and spread from location to location, typically without user knowledge or permission. Viruses are written by programmers with malicious intent to annoy computer users.
- Worms are similar to viruses in that they make copies of themselves, but differ in that they need not attach to particular files or sectors at all. Once a worm is executed, it seeks other systems - rather than parts of systems - to infect, then copy its code to them. Typically worms slow down computer systems.
- Trojan horses secretly place illegal, destructive instructions in the middle of a computer program. Once the program is run, the Trojan horse becomes active. Trojans do not replicate themselves like other viruses.
- Spyware is a program that secretly installs itself on computers and collects information about users without their knowledge. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited. They can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs.

Two sources of viral infections are:

- Sharing infected files over the intranet i.e. the internal computer network of an organisation.
- Downloading infected files from Internet sites.

You should be careful with program or file downloads from the Web. Files available on bulletin boards or public newsgroups may be infected. Software updates e.g. drivers, multimedia players, should be downloaded from the manufacturer's official website. It is important to update your anti-virus program to prevent against malware.

Using Antivirus Software

Anti-virus software is a program which protects the computer system against most viruses. Typically, such programs detect the presence of viruses in a computer and in most cases remove (or disinfect) any files infected by viruses.

Different users may have different anti-virus programs. You can follow these generic steps to scan specific drives, folders and files for viruses.

1. Click **Start** button.
2. Highlight **All Programs**.
3. Highlight the antivirus program. A submenu will be displayed.
4. Select the appropriate scanning option.
5. Follow any other steps.

Unfortunately, new viruses are being developed all the time. Thus, if the anti-virus program is not updated on a regular basis it will not be able to detect new virus types and variants. When you install an update, new entries are added to the software's virus definitions database so that suspect files can be recognised and dealt with. Most anti-virus programs are updated automatically when you connect your computer to Internet.