Day 7	**Health and Safety** **+** **Security Issues** **+** **Privacy Issues** **+** **Computer Viruses** **+** **Copyright**	**22-11-2015** **23 -11-2015**

Health and Safety

Ergonomics بيئة العمل

The term ergonomics refers to the relationship between workers and their working environment. The following aspects of the working environment should be taken into account when assessing whether or not a working environment is suitable for computer operation:

- Adequate lighting.
- Adequate ventilation.
- Monitor filters/anti-glare screens if required.
- A comfortable chair for the user.
- A mouse mat or suitable equivalent surface.
- Suitably positioned keyboard, not too far away from the user.
- Frequent breaks away from the computer (10mins after every 50mins work).
- Swivel chairs and roomy desks are comfortable and safe.

Health Issues

Injuries common in an IT environment are:

- Aches and pains (especially to the back) due to bad posture when seated for long periods.
- **R**epetitive **S**train **I**njury (**RSI**) caused by poor ergonomics combined with repeated movements of the same joints, e.g. wrist, over a long period of time.
- Eye strain which can be caused by glare or flickering from a VDU and by not taking regular visual breaks (10 minutes every hour is recommended) away from the screen.

Security Issues

Backing Up

A good practice for a PC operator is to save their work to permanent storage (HDD or file server) after regular, short periods. This ensures that if a power cut occurs, only the data produced since the last save is lost. Certain software applications offer the facility to perform this task automatically.

Regardless protecting data against loss due to power failure, serious hardware fault, physical damage, fire or infection by computer virus or theft; the organization needs to consider the financial losses.

The loss of work files of a business user, large or small is very harmful. So, the backing up files that may be carried out hourly, daily, weekly are needed.

Backing Up (cont'd)

The fundamental reason for backing up files is to ensure that they cannot be lost, or completely destroyed, while saved on the hard drive of the PC or the file server. It is, therefore, not totally secure to keep the backing store in the same room, or even building, as the source material because of the risk of fire. All backup media should be kept in a storage environment, which is theft-proof, fireproof and waterproof.

Privacy Issues

If there is any need to consider the content of certain files as being sensitive or confidential, the use of password protection should be used to prevent unauthorised persons accessing, viewing or editing the data. A password typically acts as a user's personal entry code to his PC. Passwords should be changed regularly, to prevent the possibility of misuse by unauthorised individuals.

As well as password protection, most organisations or systems would require the use of a user **I**dentity **D**ocument (otherwise referred to as a user-name or log-in name). This is another level of access code that provides evidence of a user's right to access certain areas of a network or system. A number of users might be given the same user **ID**.

Privacy Issues (cont'd)

As part of overall security, persons should be aware of the sensitive nature of information stored in portable appliances such as laptops, PDAs and mobile phones. If such a device was lost or stolen, not only could confidential files fall into the wrong hands but personal information (addresses, phone numbers etc.) could be misused by the finder and contact details could be lost to the company. All such devices should be kept safe at all times and password protection should be applied wherever available, also, as much of the material as possible should be included in any backup version.

Computer Viruses

A computer virus is a malicious piece of programming that is written specifically to cause harm to other computer programs or files. Virus looks like an infection, being passed from program to program, file to file, PC to PC or system to system.

Viruses can cause many levels of harm to a computer system. for example if a user typed text into a word processed document on an infected computer, certain letters or words might appear on screen in an unexpected text format.

Virus Types

A virus might be dormant until a certain date or until the computer has been restarted a certain number of times, and then become active. This type of virus is variously known as **a time bomb** or **logic bomb**. It could then destroy the entire file structure as laid down on the HDD and makes the HDD completely useless. If this type of virus infected a network, the effect could be catastrophic.

Macro viruses are those that are added to executable files within an application. The most common of these can occur within the template files in Microsoft Word and Excel. This is why a user is sometimes given the option of opening such a file with macros disabled. If the macro facility can't run, neither can any virus that might be within it!

A worm is a type of virus that does not affect files, but replicates itself within a system so many times that it simply stops the system resources.

A Trojan Horse virus is so called because it is masked as a file that a user would be particularly tempted to open, e.g. a game or a graphics file.

Currently, the most common type of virus is one that arrives in an ***e-mail attachment***.

It therefore follows that the only pathways available to viruses are via input devices such as floppy disks, CDs or DVDs or the Internet. If genuine application software from original sources only is installed on a PC; should be no danger.

Anti-virus measures مكافحة الفيروسات

Taking certain basic safety precautions will reduce the chances of infection:

- Install reliable anti-virus software and update it regularly.
- Regular scans of the entire system.
- Scan any removable disk that is placed in a drive on the system before installing or opening any files from it.
- Be aware about the source of any software you use!
- Save any files downloaded from the Internet, either to a floppy disk or to the HDD and scan them with anti-virus software before opening them.
- Be aware of any e-mail messages from an unknown source.

Anti-virus software

Every computer system in use now should have an anti-virus program installed. Virus writers modify existing viruses and create new examples almost every day. **This means that once a user has installed an anti-virus program it should be updated immediately**. Updating is typically done via the Internet.

An anti-virus program purchased and installed 18 months previously and never updated, is virtually useless!

Copyright

Software copyright legislation

This exists to give the authors/developers of software the same legal protection as the authors of published.

If a person purchases a book, music CD, a computer program, a game, application software or an operating system; copyright law prohibits them from copying that material in any way without the permission of the author.

End User Agreement

In order to use software application for all employees, multi-user site licences can be purchased. An organisation might use Microsoft Office 2000 as its standard software package in an environment where 25 employees could be expected to use the program at any one time.

When a piece of software is installed onto a computer, there is usually a point in the installation process where the user has to enter its own name and/or their company name. There is another stage when the user has to signify (usually by ticking a check box) that they have read and accepted the End User Agreement. This is the document mentioned earlier, which details exactly what the user is permitted to do with the software. The End User Agreement is usually displayed in a scrolling dialog box at the same stage as the indication of acceptance by the user. Without this acceptance, installation will not proceed.

Product ID [Product Identification number]

Each program has its own registration number known as the Product ID.

Shareware is a type of software is obtained and distributed free of charge and installed for a pre-determined trial period, typically 30 days.

Another type of shareware is software that is available free of initial fee, but is not the fully functioning version of the program. But the user must then pay to receive the full version.