



# Ethiopian TVET-System



## **IT SUPPORT SERVICE LEVEL II** Based on May 2011 Occupational Standards

October, 2019



**Module Title: Caring for Network and Computer Hardware**

**TTLM Code: ICT ITS2TTLM 1019v1**

**This module includes the following Learning Guides**

**LG27: Identify computer hardware components**

**LG Code: EIS ITS2 M07 1019 LO1-LG27**

**LG28:-Hardware requirements with specified manufacturers**

**LG Code: EIS ITS2 M07 1019 LO2-LG28**

**LG29: Monitor threats to the network**

**LG Code: EISITS2M071019LO3-LG29**

**LG30: Establish maintenance practices**

**LG Code: EIS ITS2 M07 1019 LO4-LG30**



<b>ICT ITS1</b>	Version:01	Page No.0
	Copyright: Ethiopia Federal TVET Agency	



<b>Instruction Sheet</b>	<b>LG27: Identify computer hardware components</b>
--------------------------	--

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics –

- Identifying external hardware components and peripherals
- Identifying internal hardware components.
- Reviewing, recording and applying Requirements specifying by hardware manufacturers
- Determining and recording quality standard of hardware and peripherals
- Determining and establishing relationship of hardware and software components
- Determining, recording and applying Safe work practices

This guide will also assist you to attain the learning outcome stated in the cover page.

Specifically, upon completion of this Learning Guide, you will be able to –

- External hardware components and peripherals are identified based on business requirement
- Internal hardware components are identified as needed
- Requirements specified by hardware manufacturers are reviewed, recorded and applied where appropriate.
- Quality standards of hardware components and associated peripherals are determined and recorded
- Relationship of computer hardware and software is determined and established for proper functioning of the system
- Safe work practices are determined, recorded and applied, taking into account legal and manufacturer requirements

### Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 5.
3. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3, Sheet 4, Sheet 5 and Sheet 6” in **page 1, 4, 9, 19, 22, and 44** respectively.
4. Accomplish the “Self-check 1, Self-check 2, Self-check 3, Self-check 4, Self-check 5 and Self-check 6” in **page 2, 7, 16, 20, 42 and 46** respectively

<b>ICT ITS1</b>	Version:01	Page No.0
	Copyright: Ethiopia Federal TVET Agency	



<b>ICT ITS1</b>	Version:01	Page No.1
	Copyright: Ethiopia Federal TVET Agency	

**1.1. Hardware**

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners etc.

**Basic Components**

- **Case or Tower** - This is the plastic box that contains the computer. Housed in the case, you will find the floppy drive, CD R OM drive, and the main components of the computer. Some of these are the hard drive, motherboard and the processor chip (CPU). The case keeps them neatly and safely together.
- **Monitor or Screen** - This is the TV-type screen on which you see the work you're doing on your computer.
- **Mouse** - The mouse allows you to move, select and click on objects.
- **Keyboard** - The keyboard is used to type in information and operate the computer.
- **Speakers** - Sometimes speakers are connected to the computer so that you can hear music and sound.
- **Microphone** - A microphone can provide a way to talk through or to the computer.
- **Printer** - A device that makes a printed copy of your work on a sheet of paper.
- **A scanner** is a device that captures text or illustrations on paper and converts the information into a form the computer can use. One of the most common kinds of scanners is called a flatbed scanner. It has a glass surface on which you lay paper, magazines, or other documents that you want to scan. Sometimes scanners can be manufactured so that they are combined with a printer thus can also be used as a photocopier and fax machine.
- **Digital cameras** store images digitally onto a storage device, either a memory card or a floppy disk, rather than recording them on film. Once a picture has been taken, it can be downloaded to a computer system, and then manipulated or printed.
- **USB flash drive**:-A small, portable device that plugs into a computer's USB port and operates as a portable hard drive. USB flash drives are considered to be an ideal method



to transport data, as they are small enough to be carried in a pocket and can plug into any computer with a USB drive. Other names for flash drives are thumb drives, pen drives or USB drives.

Self Check 1	Written Test
--------------	--------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

Match the most appropriate peripheral device to A column from B column.

### Column A

- \_\_\_\_\_ 1. Mouse
- \_\_\_\_\_ 2. Speakers
- \_\_\_\_\_ 3. Keyboard
- \_\_\_\_\_ 4. Joystick
- \_\_\_\_\_ 5. Monitor
- \_\_\_\_\_ 6. Microphones
- \_\_\_\_\_ 7. Digital Camera
- \_\_\_\_\_ 8. Printers
- \_\_\_\_\_ 9. scanner
- \_\_\_\_\_ 10. Case

### Column B

- A. The TV-type screen on which you see the work you're doing on your computer.
- B. Select and click on objects
- C. The plastic box that contains the computer
- D. Used to type in information and operate the computer.
- E. Store images digitally onto a storage device
- F. That used for hear music and sound.
- G. A device that captures text or illustrations on paper and converts the information into a form the computer can use.
- H. A device that makes a printed copy of your work on a sheet of paper.
- I. can provide a way to talk through or to the computer
- J. Game port



**Note: Satisfactory rating - 5 points**

**Unsatisfactory - below 5 points**

You can ask your teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

### List of Reference Materials

#### 1. BOOKS

2. <https://training.gov.au/Training/Details/ICTSAS506>
3. [web1.keira-h.schools.nsw.edu.au/faculties/IT](http://web1.keira-h.schools.nsw.edu.au/faculties/IT)





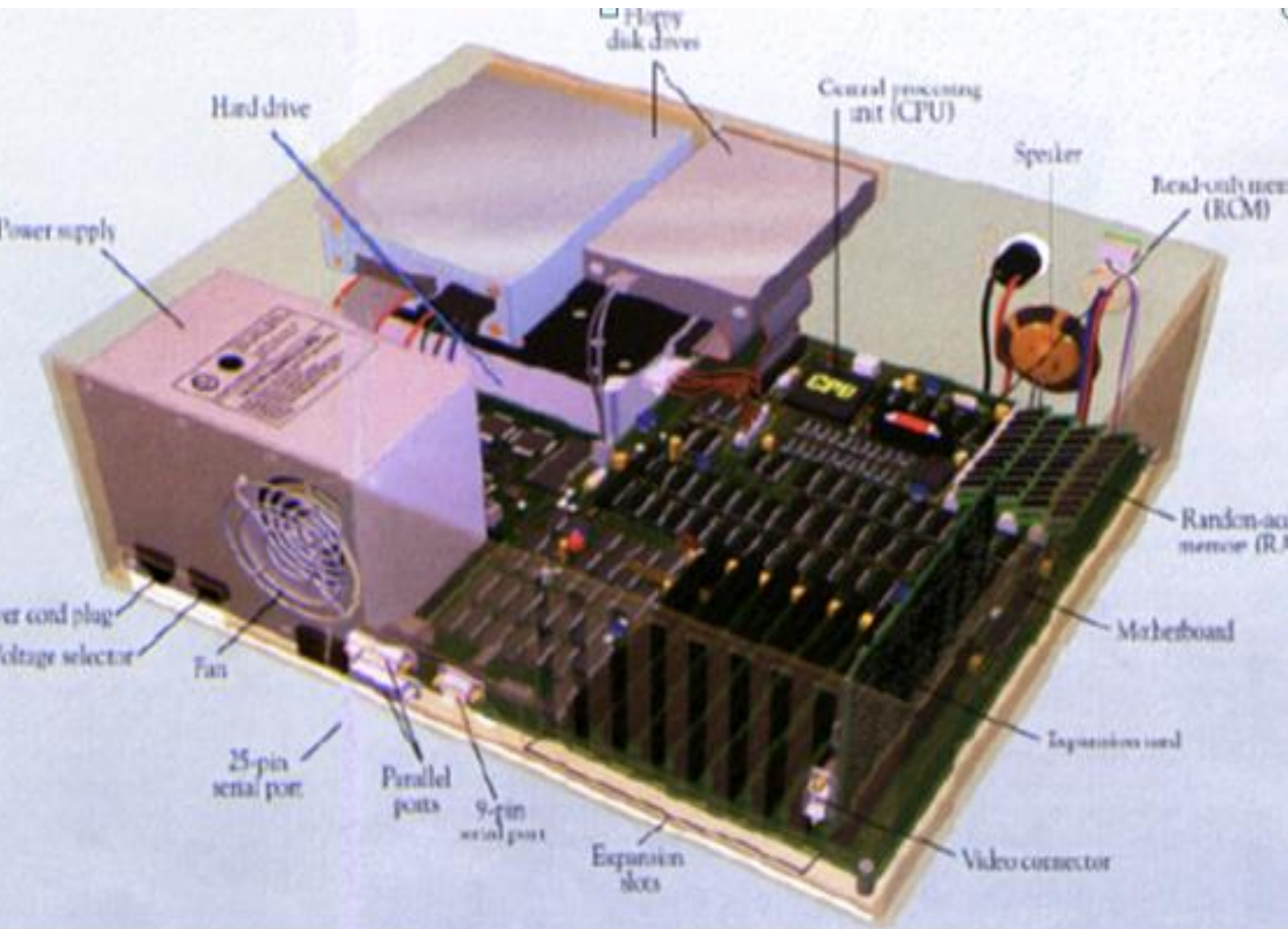
## Information Sheet – 2

## Identifying internal hardware components

### 1.1. Introduction

The internal hardware parts of a computer are often referred to as components, while external hardware devices are usually called peripherals. Together, they all fall under the category of computer hardware. Software, on the other hand, consists of the programs and applications that run on computers. Because software runs on computer hardware, software programs often have system requirements that list the minimum hardware required for the software to run.

**Note:** *Peripheral devices are the devices that are attached to the computer's system unit*





## INTERNAL COMPONENTS











	<p><b>Power Supply</b> A power supply changes normal household electricity into electricity that a computer can use.</p>		<p><b>Hard Drive</b> A hard drive is the primary device that a computer uses to store information</p>
	<p><b>Expansion Card</b> An expansion card lets you add new features to a computer.</p>		<p><b>Expansion Slot</b> An expansion slot is a socket on the motherboard that expansion cards plug into.</p>
	<p><b>Motherboard</b> The motherboard is the main circuit board of a computer. All computer components attached to the motherboard.</p>		<p><b>Central Processing Unit (CPU)</b> The CPU processes instructions, performs calculations and manages the flow of information through a computer.</p>
	<p><b>Random Access Memory (RAM)</b> RAM temporarily stores information inside a computer. The Information is lost when computer is turned off.</p>		<p><b>CD-ROM</b> A CD-ROM drive reads information stored in compact discs (CDs).</p>
	<p><b>Drive Bay</b> A drive bay is the space inside the computer case where a hard drive, floppy drive or CD-ROM drive sits.</p>		<p><b>Floppy Drive</b> A floppy drive stores and retrieves information on floppy disks.</p>

Figure 1.2:- Internal component



<b>ICT ITS1</b>	Version:01	Page No.7
	Copyright: Ethiopia Federal TVET Agency	



## COMPONENT FUNCTIONS

- **CPU:** The CPU is the brains of the computer. All information goes through the CPU to be processed. The latest CPUs execute many millions of instructions per second.
- **MEMORY:** Memory is where the information is stored.
- **RAM:** Random Access Memory stores programs and data as it is used. The information in RAM is lost when the power is turned off.
- **ROM:** Read Only Memory stores start up and basic operating information.
- **DISKS:** Disks are where large amounts of information are stored, even when the power is off.
- **Floppy Disks** - Information can be written to and read from floppy disks. The advantage of floppy disks is that they can be removed from the computer and the data taken to another machine.
- **Hard disks** - Hard disks are not removable like floppy disks, but hold more information.
- **CD ROMs** - Compact Disk Read Only Memory. They are useful for storing large amounts of data. A CD ROM holds about 650 MB of data and is removable.
- **Input/Output Components** : Allow a computer to communicate with the outside world. Following are some examples of Input/ Output devices.
- **Keyboard** is used to enter information from the user to the computer.
- **Monitors** are used to display information.
- **Video controller** is a board in the computer that controls the monitor. It translates the data in the video memory into symbols on the monitor .
- **Parallel/Serial ports** allow the computer to send data to and receive data from printers, modems, etc.
- **Mouse and Joystick** are used to input positional information to the computer.
- **Network Interface Card** – A NIC connects the computer to a network. Networks are a high - speed method of transferring data from one computer to another.

ICT ITS1	Version:01	Page No.8
	Copyright: Ethiopia Federal TVET Agency	



Self Check 2

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications-  
feel free to ask your teacher.

Match the most appropriate peripheral device to A column from B column.

**Column A**

- \_\_\_\_\_ 1.Memory
- \_\_\_\_\_ 2.CPU
- \_\_\_\_\_ 3.Video controller
- \_\_\_\_\_ 3.DISKS
- \_\_\_\_\_ 1Network Interface

**Column B**

- A. The brains of the computer
- B. Connects the computer to a network
- C. Are not removable like floppy disks, but hold more information
- D. Where the information is stored
- E. A board in the computer that controls the monitor

**Note: Satisfactory rating – 3 points**

**Unsatisfactory - below 3 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = _____
Rating: _____



## List of Reference Materials

1. **BOOKS**
2. <https://training.gov.au/Training/Details/ICTSAS506>
3. [web1.keira-h.schools.nsw.edu.au/faculties/IT](http://web1.keira-h.schools.nsw.edu.au/faculties/IT)



## Information Sheet – 3

## Reviewing ,recording and applying Requirements specifying by hardware manufacturers

### 3.1. Access point

#### Internet Access

- There are several ways to obtain Internet access.
- The type chosen often depends on the cost as well as what technologies are available in the area you are located.
  - XDSL Internet Access
  - Cable Internet Access
  - Satellite Internet Access
  - Wireless Internet Access
  - POTS(Plain Old Telephone Service) Internet Access

#### XDSL Internet Access

- DSL is an Internet access method that uses a standard phone line to provide high-speed Internet access.
- DSL offers phone and data transmissions over a standard phone connection.
- High-speed Internet access;
- Less expensive than technologies such as ISDN

With DSL a different frequency can be used for digital and analog signals, which means that you can talk to a friend on the phone while you're uploading data.

#### DSL's staggering number of flavors

- **Asymmetric DSL (ADSL)** The word asymmetric describes different channels on the line: One channel is responsible for analog traffic, the second channel is used to provide upload access, and the third channel is used for downloads. With ADSL, downloads are faster than uploads.

ICT ITS1	Version:01	Page No.11
	Copyright: Ethiopia Federal TVET Agency	



- **Symmetric DSL (SDSL)** - offers the same speeds for uploads and for downloads, making it most suitable for web hosting, intranets, and ecommerce. It is not widely implemented in the home/small business environment and cannot share a phone line.
- **ISDN DSL (IDSL)** - a symmetric type of DSL commonly used in environments where SDSL and ADSL are unavailable. IDSL does not support analog phones.
- **Rate Adaptive DSL (RADSL)** - a variation on ADSL that can modify its transmission speeds based on the signal quality. RADSL supports line sharing.
- **Very High Bit Rate DSL (VHDSL)** - VHDSL is an asymmetric version of DSL and can share a telephone line.
- **High Bit Rate DSL (HDSL)** - HDSL is a symmetric technology that offers identical transmission rates in both directions. HDSL does not allow line sharing with analog phones.
- Why are there are so many DSL variations?
  - Each flavor of DSL is aimed at a different user, business, or application.
- What is the major differences?
  - DSL options can be a **shared** or **dedicated** link. ADSL for instance is a shared DSL connection while SDSL is not (or dedicated link).
  - A dedicated DSL line is not used for regular voice transmissions.

ICT ITS1	Version:01	Page No.12
	Copyright: Ethiopia Federal TVET Agency	



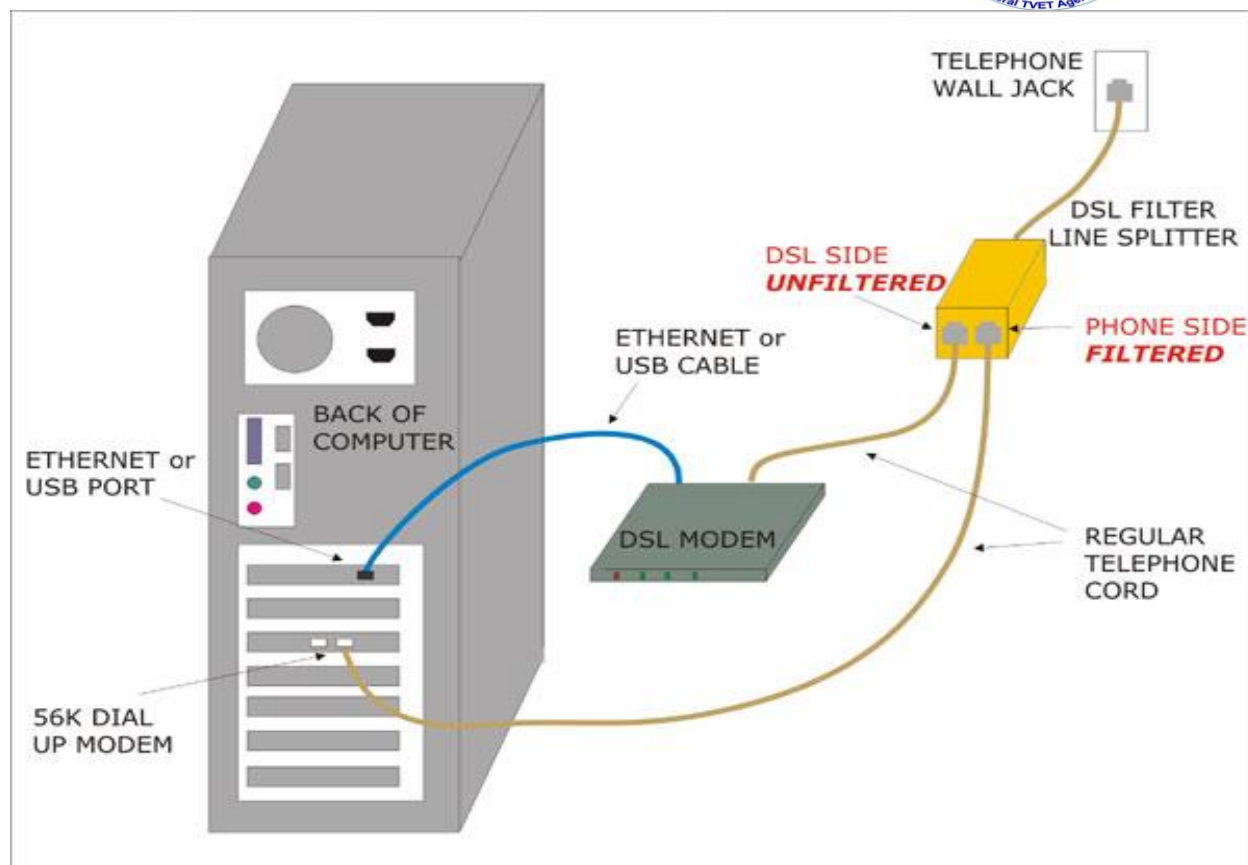


Figure 1.3:- DSL Internet Access



## Cable Internet Access

- Cable Internet access is an always-on Internet access method available in areas that have digital cable television.
- Cable Internet access is attractive to many small businesses and home office users because it is both inexpensive and reliable.
- Connectivity is achieved by using a device called a **cable modem**; it has a coaxial connection for connecting to the provider's outlet and an unshielded twisted-pair (UTP) connection for connection directly to a system or to a hub or switch.
- Most cable modems supply a 10Mbps Ethernet connection for the home LAN, although the actual Internet connection ranges from 1.5Mbps to 3Mbps.
- One of the biggest disadvantages of cable access is the fact that you share the available bandwidth with everyone else in your cable area.
- As a result, during peak times, performance of a cable link might be poorer than in low-use periods.

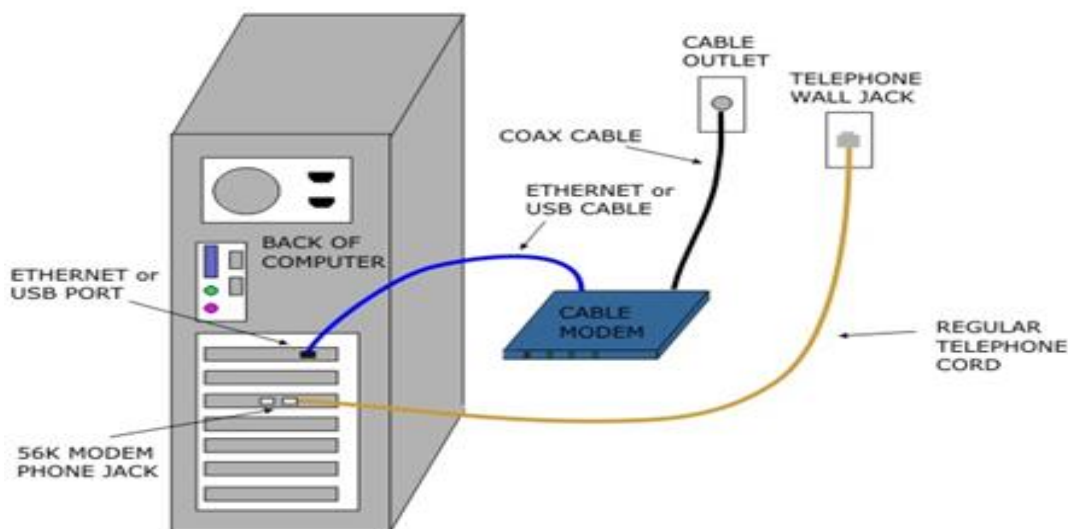


Figure 1.4:- Cable Internet Access

ICT ITS1	Version:01	Page No.14
	Copyright: Ethiopia Federal TVET Agency	



Feature	Cable Internet	DSL Internet
Bandwidth/ Speed	The theoretical maximum cable speed of 30Mbps downstream, aside, in practical use the rate is somewhere between 300 and 700Kbps downstream and a 128 connection.	DSL lists speeds from to 384Kbps to 6.0Mbps depending on the type of DSL used and whom you ask. DSL offers 128Kbps upstream transfers.
Connection type	Cable Internet uses a shared connection. You share the connection with others in your area. This can affect bandwidth performance during peak usage times.	DSL bandwidth is dedicated and not shared.
Distance factors	With cable Internet distance is not a concern. Subscribers maintain the same speeds regardless of the distance from the Internet provider.	DSL speeds degrade as the distance from the ISP increases. The farther you are, the more overall speed deteriorates.
Security	The shared nature of cable Internet make it an increased security risk. Security risks include eavesdropping, tampering, service theft and more.	DSL is more secure because it offers a dedicated link to the ISP. The dedicated link helps protect against attacks associated with a shared connection.

Table 1.1. Cable Internet and DSL Internet



## Satellite Internet Access

- DSL and cable Internet access are not offered everywhere.
- Satellite Internet offers an **always-on** connection with theoretical speeds advertised anywhere from 512Kbps upload speeds to 2048Kbps download speeds, considerably faster than a 56K dial-up connection.
- One primary drawback to satellite Internet is the cost, and even with the high price tag, it is not as fast as DSL or cable modem.
- As with other wireless technologies, **atmospheric conditions** can significantly affect the performance of satellite Internet access.
- Greatest advantage is its **portability**.

### Types of Satellite Internet

- Two different types of Internet satellite services are deployed: **one-way** and **two-way** systems.
- A one-way satellite system requires a satellite card and a satellite dish installed at the end user's site; this system works by sending outgoing requests on one link using a phone line, with inbound traffic returning on the satellite link.
- A two-way satellite system, on the other hand, provides data paths for both upstream and downstream data. Like a one-way system, a two-way system also uses a satellite card and a satellite dish installed at the end user's site; bidirectional communication occurs directly between the end user's node and the satellite.

ICT ITS1	Version:01	Page No.16
	Copyright: Ethiopia Federal TVET Agency	



Figure 1.5 **Satellite Internet Access**

### Wireless Internet Access

- Nowadays it is becoming increasingly common to see people surfing the Web in many different public places.
- This is made possible by subscribing to a wireless Internet service provider (WISP) or connecting to a company's local wireless router.

<b>ICT ITS1</b>	Version:01	Page No.17
	Copyright: Ethiopia Federal TVET Agency	



- A WISP provides public wireless Internet access known as *hotspots*.
- A hotspot is created using one or many wireless access points near the hotspot location.
- Airports, hotels, and coffee shops will advertise that they offer Internet access for customers or clients.

### **POTS(Plain Old Telephone Service) Internet Access**

- The most popular means of connecting to the Internet or a remote network may still be the good old telephone line and modem.
- Because the same line used for a household phone is used for dial-up access, it is referred to as the **POTS** (Plain Old Telephone Service) method of access.
- Although many parts of the world are served by broadband providers, many people still connect with a modem.
- Internet access through a phone system requires two things: a **modem** and a **dial-up access account** through an ISP.
- A big consideration for dial-up Internet access is how many lines the ISP has. ISPs never have the same number of lines as subscribers; instead, they work on a first-come, first-served basis for dial-up clients.
- This means that on occasion, users get busy signals when they try to connect.

<b>ICT ITS1</b>	Version:01	Page No.18
	Copyright: Ethiopia Federal TVET Agency	



Self Check 3	Written Test
--------------	--------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

Match the most appropriate peripheral device to A column from B column.

### Column A

- \_\_\_\_\_ 1.XDSL Internet Access
- \_\_\_\_\_ 2.Cable Internet Access
- \_\_\_\_\_ 3.Satellite Internet Access
- \_\_\_\_\_ 4.Wireless Internet Access
- \_\_\_\_\_ 5.(Plain Old Telephone Service)  
Internet Access

### Column B

- A. It is becoming increasingly common to see people surfing the Web in many different public places.
- B. The most popular means of connecting to the Internet or a remote network may still be the good old telephone line and modem.
- C. offers an always-on connection with theoretical speeds advertised anywhere from 512Kbps upload speeds to 2048Kbps download speeds, considerably faster than a 56K dial-up connection.
- D. An always-on Internet access method available in areas that have digital cable television.
- E. An Internet access method that uses a standard phone line to provide high-speed Internet access.



**Note: Satisfactory rating – 3 points**

**Unsatisfactory - below 3 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = _____
Rating: _____





## List of Reference Materials

1. **BOOKS**
2. <https://training.gov.au/Training/Details/ICTSAS506>
3. [web1.keira-h.schools.nsw.edu.au/faculties/IT](http://web1.keira-h.schools.nsw.edu.au/faculties/IT)



## Information Sheet – 4

Determining and recording quality standard of hardware and peripherals

### 4.1. System specifications

It is important to find out the specifications of the computer system you are planning to connect the peripheral device to. Many newer types of peripheral devices require a specific amount of memory, CPU speed, hard disk space, and may only be compatible with certain operating systems.

You also need to be aware of the peripheral's system requirements. The manual for the peripheral device as well as the manufacturer's website will help you determine the minimum system specifications.

#### Compatibility

Compatibility is the ability of a system or a product to work with other systems or products without special effort on the part of the customer. One way products achieve interoperability is to comply with industry interface standards. For example, a memory module is compatible with a motherboard because the manufacturer of the memory module and the motherboard both work to the same industry standard.

#### Technical specifications

Once the business requirements have been considered, the technical specifications of the hardware device need to be evaluated. Areas for evaluation include the following:

- processing speed of the CPU
- storage capacity of the hard drive
- size of memory (RAM)
- software capabilities
- compatibility with existing systems
- upgradeability

The technical specifications to be considered will depend on the computer hardware device to be purchased. For example, technical specifications to be considered for a printer include:

- interface – USB or network
- resolution – measured in dots per inch

ICT ITS1	Version:01	Page No.22
	Copyright: Ethiopia Federal TVET Agency	



- printing speed – measured in pages per minute
- memory
- paper capacity



Self Check 4

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

Match the most appropriate peripheral device to A column from B column.

**Column A**

- \_\_\_\_\_ 1. Interface
- \_\_\_\_\_ 2. Resolution
- \_\_\_\_\_ 3. printing speed
- \_\_\_\_\_ 4. storage capacity
- \_\_\_\_\_ 5. processing speed

**Column B**

- A. measured in pages per minute
- B. USB or network
- C. measured in dots per inch
- D. CPU
- E. Hard drive

**Note: Satisfactory rating – 3 points**

**Unsatisfactory - below 3 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_



## List of Reference Materials

### 1. BOOKS

2. <https://training.gov.au/Training/Details/ICTSAS506>
3. [web1.keira-h.schools.nsw.edu.au/faculties/IT](http://web1.keira-h.schools.nsw.edu.au/faculties/IT)

ICT ITS1	Version:01	Page No.1
	Copyright: Ethiopia Federal TVET Agency	



## Information Sheet – 5

## Determining and establishing relationship of hardware and software components

### 4.1. Introduction

When caring for computer equipment you will inevitably be faced with a computer, or peripheral, that is not operating as it should. You will be looked upon to provide the answer to ‘What’s wrong with it?’. In order for you to answer that question, you will need to know a basic diagnostic approach to fault finding. In this section we will examine what a system usually does when nothing is wrong, list some of the typical faults encountered and what to do about it, and what to do if you can’t fix it. If you are not able to effect repairs then you should be able to give the user some indication on how long their system will be down.

Firstly, let’s look at what normally happens, before looking at what can go wrong.

#### Booting up

##### The POST

When first turning the computer on, you will notice that there are certain lights flashing, beeping sounds and text displayed on the screen. When power is applied to a computer system, the first thing that happens is that the computer performs a Power On Self Test, commonly called a POST. After performing this self-check, the system will try to load an operating system. Loading the operating system was traditionally known as loading the bootstrap loader, or pulling the system up by the boot-straps. While the terminology has been dropped, we still use the term ‘Booting Up’ to refer to starting the system.

The BIOS (Basic Input Output System) is responsible to perform the POST. The BIOS is a program that is built-in to the motherboard and is responsible for the low level operations of the hardware, such as placing data from a hard disk and writing it into RAM (Random Access Memory), or sending video output

ICT ITS1	Version:01	Page No.2
	Copyright: Ethiopia Federal TVET Agency	



to the video card, or handling a mouse movement, or event like a click. Without the BIOS, nothing would happen when you turn the power on.

After the initial POST, assuming that the BIOS is able to boot the system far enough to gain access to the video subsystem, it will display information about the computer system as it boots. It will also use the video system to communicate error messages. In fact, most non-critical boot problems are displayed via video error messages, as opposed to audio beep codes.

Some errors in the POST may simply generate an error message on the screen and continue, while others will halt the system until the error is dealt with. If the POST is passed successfully, then the system is ready to load an operating system.

<b>ICT ITS1</b>	Version:01	Page No.3
	Copyright: Ethiopia Federal TVET Agency	



## Loading an operating system

To load an operating system, the BIOS will seek out a boot device in a set order. A boot device is usually a hard disk drive, but may be a floppy disk, CD-ROM drive, network interface card (NIC) or USB flash disk etc. That is where the terms 'Boot Disk' and 'Disk Operating System' (DOS) are derived.

There are a number of hardware level settings that are stored on a special chip called a CMOS chip. CMOS stands for Complimentary Metal Oxide Semiconductor and is usually identified as one of the chips, with a sticker with the BIOS maker's name, on the motherboard. CMOS technology is just one type used to make semiconductors (integrated circuits) such as processors, chipset chips, DRAM, etc. CMOS has the advantage of requiring very little power, compared to some other semiconductor technologies. This is why it was chosen for this use, so that the amount of power required from the battery would be minimal, and the battery would be able to last a long time.

It is common for the terms BIOS and CMOS to be used interchangeably, even though it is not technically correct. The BIOS is the program and the CMOS is the memory that stores the BIOS settings. When a program is written to a chip it is known as firmware ie software put into hardware.

To gain access to the CMOS settings, you should see some sort of message on the screen that tells you which key to press. For example 'Press <Delete> to run Setup'. Most systems use the **Delete** key, some use **F1** or **F10** and even **Escape**. If the screen does not show any message (there is sometimes an option in CMOS to turn this off) then try each key in turn. If all else fails, then read the manufacturer's instructions.

## Boot device options

You can change the boot device order from the standard:

- Floppy disk
- Hard disk drive 0 (master hard disk)
- CD-ROM.

For instance, if you had to install an operating system from new, like *Microsoft Windows XP*, you should change the boot device order to make the CD-ROM the first boot device. This is because the operating system is usually supplied on a bootable CD-ROM disk. In fact many other operating systems are originally installed from CD-ROM disk.

ICT ITS1	Version:01	Page No.4
	Copyright: Ethiopia Federal TVET Agency	





When the operating system loads, it too may generate error messages and either continue or halt. If the error messages flash by too quickly, or the system hangs at a certain point, you can try a step-by-step boot process by pressing F8 key just after the POST.

### **The system boot sequence**

The following are the steps in a boot sequence. Of course this will vary by the manufacturer of your hardware, BIOS, etc, and especially due to the peripherals you have connected. Here is what generally happens when you turn on your system power:

- 1 The internal power supply turns on and initialises. The power supply takes some time until it can generate reliable power for the rest of the computer, and having it turn on prematurely could potentially lead to damage. Therefore, the chipset will generate a reset signal to the processor (the same as if you held the reset button down for a while on your case) until it receives the Power Good signal from the power supply.
- 2 When the reset button is released, the processor will be ready to start executing. When the processor first starts up there is nothing at all in the memory to execute. Of course processor makers know this will happen, so they pre-program the processor to always look at the same place in the system BIOS ROM for the start of the BIOS boot program.
- 3 The BIOS performs the POST. If there are any fatal errors, the boot process stops.
- 4 The BIOS looks for the video card. In particular, it looks for the video card's built in BIOS program and runs it. The system BIOS executes the video card BIOS, which initialises the video card. Most modern cards will display information on the screen about the video card. This is why on most systems you usually see something on the screen about the video card before you see the messages from the system BIOS itself.
- 5 The BIOS then looks for other devices' ROMs to see if any of them have BIOSes. Normally, the IDE/ATA hard disk BIOS will be found and executed. If any other device BIOSes are found, they are executed as well.
- 6 The BIOS displays its start-up screen.
- 7 The BIOS does more tests on the system, including the memory count-up test which you see on the screen. The BIOS will generally display a text error message on the screen if it encounters an error at this point.

<b>ICT ITS1</b>	Version:01	Page No.5
	Copyright: Ethiopia Federal TVET Agency	



- 8 The BIOS performs a 'system inventory' of sorts, doing more tests to determine what sort of hardware is in the system. Modern BIOSes have many automatic settings and can dynamically set hard drive parameters and access modes, and will determine these at roughly this time. Some will display a message on the screen for each drive they detect and configure this way. The BIOS will also now search for and label logical devices (COM and LPT ports).
- 9 The BIOS will detect and configure Plug and Play devices at this time and display a message on the screen for each one it finds.
- 10 The BIOS will display a summary screen about your system's configuration. Checking this screen of information can be helpful in diagnosing setup problems, although it can be hard to see because sometimes it flashes on the screen very quickly before scrolling off the top or behind an operating systems splash screen. Try being quick to press the <Pause> key.
- 11 The BIOS begins the search for a device to boot from.
- 12 Having identified its target boot device, the BIOS looks for boot information to start the operating system boot process. If it is searching a hard disk, it looks for a master boot record (MBR) at cylinder 0, head 0, sector 1 (the first sector on the disk); if it is searching a floppy disk, it looks at the same address on the floppy disk for a volume boot sector.
- 13 If it finds what it is looking for, the BIOS starts the process of booting the operating system, using the information in the boot sector. At this point, the code in the boot sector takes over from the BIOS. If the first device that the system tries (floppy, hard disk, etc.) is not found, the BIOS will then try the next device in the boot sequence, and continue until it finds a bootable device.
- 14 If no boot device at all can be found, the system will normally display an error message and then freeze up the system. What the error message is depends entirely on the BIOS, and can be anything from 'No boot device available' to 'No ROM BASIC—System Halted'.

When diagnosing hardware problems you will need to keep in mind the steps above, particularly for errors that halt the system from starting up.

### **Error messages**

An error message can be produced by different parts of the system, depending on how far into the boot process the system gets before it is produced. Most error messages are produced by the system BIOS,

<b>ICT ITS1</b>	Version:01	Page No.6
	Copyright: Ethiopia Federal TVET Agency	



as it is responsible for most of the functions of starting the boot process. However, other error messages are operating system specific.

Error messages that crop up while the system is operational can be generated by different sources, including the system BIOS, the operating system, hardware driver routines, or application software. It is usually possible to determine roughly what is causing the error, since application-specific messages usually mention the application that is generating them. However, error messages that crash a specific application can sometimes be caused by hardware or system problems, especially if the problem occurs in many different applications. This can make diagnosis very difficult.

Even sticking to hardware, there are many thousands of individual error messages; some are more common than others because there are only a few different BIOS companies that are used by the majority of systems in use. However, since the exact wording of an error message can be changed by the manufacturer of each system or motherboard, there are a lot of variations.

In most cases, the messages are pretty similar to each other; you may see a slightly different wording in your error message than the ones listed here, but if the messages meaning will be substantially the same. For example, 'Disk drive failure' and 'Diskette drive failure' are virtually identical messages.

You may want to consult with your owner's manual regarding some unusual messages, or to ensure that your manufacturer means the same thing with their messages compared to others.

### **BIOS beep codes**

There usually is a single quick beep sound when a system is turned on, and that often is an audible acknowledgement of a good power supply ie the Power Good signal. However, when diagnosing fatal errors in a system, knowledge of the beep codes, and their meaning, can be the key to quick repair or replacement. Unfortunately not all manufacturers use the same set of codes to mean the same error, so we will have a look at some of the most common.

### **AMI BIOS beep codes**

The American Megatrends Inc. (AMI) BIOS is one of the most popular in the personal computing world and is quite consistent in its use of beep codes, across its many different versions.

<b>Beep Code</b>	<b>Meaning</b>
------------------	----------------



1 beep	There is a problem in the system memory or the motherboard.
2 beeps	Memory parity error. The parity circuit is not working properly.
3 beeps	Base 64K RAM failure
4 beeps	System timer not operational. There is problem with the timer(s) that control functions on the motherboard.
5 beeps	The system CPU has failed.
6 beeps	Keyboard controller failure.
7 beeps	Virtual mode exception error.
8 beeps	Video memory error. The BIOS cannot write to the frame buffer memory on the video card.
9 beeps	ROM checksum error. The BIOS ROM chip on the motherboard is likely faulty.
10 beeps	CMOS checksum error. Something on the motherboard is causing an error when trying to interact with the CMOS.
Continuous beeping	A problem with the memory or video.

Table 1.2. AMI BIOS beep codes



## Phoenix BIOS beep codes

Phoenix uses sequences of beeps to indicate problems. The '-' between each number below indicates a pause between each beep sequence. For example, 1-2-3 indicates one beep, followed by a pause and two beeps, followed by a pause and three beeps. Phoenix version before 4.x use 3-beep codes, while Phoenix versions starting with 4.x use 4-beep codes. This list is by no means comprehensive.

4- Beep Code	Meaning
1-1-1-3	Faulty CPU/motherboard.
1-1-2-1	Faulty CPU/motherboard.
1-1-2-3	Faulty motherboard or one of its components.
1-1-3-2	
1-1-3-3	
1-2-1-2	
1-1-3-2	Failure in the first 64K of memory.
1-1-4-1	Level 2 cache error.
1-1-4-3	I/O port error.
1-2-1-1	Power management error.
1-2-2-1	Keyboard controller failure.
1-2-2-3	BIOS ROM error.
1-2-3-1	System timer error.
1-2-3-3	DMA error.
1-2-4-1	IRQ controller error.
1-3-1-1	DRAM refresh error.
1-3-3-1	Extended memory error.



4- Beep Code	Meaning
2-3-1-1 2-3-3-3	
1-3-3-3 1-3-4-1 1-3-4-3 2-2-4-1	Error in first 1MB of system memory.
1-4-1-3 1-4-2-4	CPU error.
2-1-2-3	BIOS ROM error.
2-1-3-1 2-1-3-3	Video system failure.
2-1-1-3 2-1-2-1 2-2-3-1	IRQ failure.
2-1-2-3	BIOS ROM error.
2-1-2-4	I/O port failure.
2-1-4-3 2-2-1-1	Video card failure.
2-3-4-1 2-3-4-3 2-3-4-1 2-3-4-3 2-4-1-1	Motherboard or video card failure.



4- Beep Code	Meaning
3-1-4-1 3-2-1-1 3-2-1-2	Floppy drive or hard drive failure.
3-3-1-1	Real Time Clock error.

Table 1.3 Phoenix BIOS beep codes

### Award BIOS beep codes

Award BIOSes do not have many error beep codes, instead most errors are reported on the screen.

### Typical hardware level errors

While the range of possibilities is enormous when it comes to errors and computing problems, there are a few typical errors. For each of the errors, there may be a simple solution, or at least a way of determining the actual cause of the problem. Let's look at some of them:

### System appears dead

Listen to the power supply and determine if the internal fan starts up. If the fan does not start up then the cause of the problem could be:

- The system is not plugged into a power outlet, or the outlet has no power.
- The power supply unit is faulty.
- There is an internal short circuit and the fan does not start as a protective measure.
- The computer is dead!

### No video

No video appears on the screen when the system is performing its POST. Often an audible beep is heard if the BIOS detects the video error, but other likely causes are:

- Video card is faulty — swap it out with a known good card.

ICT ITS1	Version:01	Page No.11
	Copyright: Ethiopia Federal TVET Agency	



- There is a fault in the motherboard.
- The video card is not inserted correctly.
- The monitor is turned off or has no power.

### **No boot device or unable to boot**

The system could not find a bootable device; the most likely cause is the hard disk drive. The system summary screen is the first place to check. If the hard disk is listed as a detected device, then the problem may be a logical and not physical problem. Things to consider are:

- Missing boot files — they may have been deleted by the user.
- A virus has caused damage to the boot files or has corrupted the file system or Master Boot Record (MBR).
- A common mistake is a floppy disk being left in the drive.
- Cables not connected to hard disk drive properly.

<b>ICT ITS1</b>	Version:01	Page No.12
	Copyright: Ethiopia Federal TVET Agency	





### **Failure to read hard disk drive**

This usually means that there is a serious problem with the drive which may be physical or logical. A physical problem would mean the drive was unserviceable, whereas a logical problem may mean the drive and its contents could be recovered by:

- Running a disk checking program like scandisk, fsck, Norton's Disk Doctor or some other program appropriate to the operating system.
- Reinstalling the operating system making sure the drive is formatted. If the option allows it, perform a full format and not a quick format. A full format will make a thorough check of the drive for faulty sectors.
- The cable may be faulty or not connected to the hard disk drive properly.

### **CD-ROM or DVD-ROM drive not reading disks**

It is common for copied disks to be difficult to be read in standard CD/DVD-ROM drives. Often the drive (CD/DVD Read Write drive, a.k.a. burner) that was used to copy the disk will be able to read the contents, unless the disk is totally unserviceable. Other possibilities are:

- The copying process was never complete and the disk session not closed off. Check the setting on the software in use.
- General poor quality disks or CD/DVD burner.
- Disk dirty or in need of cleaning.
- Faulty drive — when CD-ROM drives first came onto the market, the quality was poor and it seemed as though they were a disposable item. These days the quality and reliability seems much improved.

### **Floppy drive errors**

Floppy disks are notable for their unreliability. This is one reason why it is important to have more than one copy of a disk, or its contents. Things to consider:

- Try the disk in another drive or two, if it can be read then the problem is likely the floppy disk drive (FDD) and not the disk.
- The cable to the drive has not been connected properly. Most cables to floppy disk drives can be connected to two drives. To distinguish between the first (A) and second (B) drive there is a twist

<b>ICT ITS1</b>	Version:01	Page No.13
	Copyright: Ethiopia Federal TVET Agency	



in the wires of the cable. If there is only a single drive (most common) and the cable is not connected at the end of the cable (past the twist) then a drive error message is typical.

- The floppy disk has not been formatted to this operating system.

### **Unable to print**

Most current printers come with a high degree of intelligence built in and can detect errors like cable not connected, printer offline, out of paper, out of toner/ink etc. Things to consider:

- Read the LCD display (if the printer has one) or check the status lights are displaying what they should for normal operation.
- Check the print manager software of the operating system to see if the printer is being shown as connected and on-line. If it is not on-line or shown as connected, then it may be a hardware problem.
- Change the cable.
- Perform a self test on the printer using the LCD display or options on the printer panel. If it performs the test properly then try the options available in the printer control of your operating system.

### **No network connectivity**

The likely cause of networking problems can be many and varied. Without delving into the finer details of networking, the easiest option to try is to change the network cable and check the status lights that are on both the network interface card (NIC) and the hub/switch/router at the other end. If there is activity then the likely cause is not hardware. You can also try switching off, or resetting, the hub/switch/router.

### **System hangs (locks up)**

One of the most difficult to problems with personal computers occurs when it appears as though a system is not responding to any user input (key press, mouse movement etc.). The likely causes are many and varied but a few possibilities are:

- Faulty memory (RAM) — you could turn memory testing on in CMOS settings which may confirm the problem, or perform a rigorous test using third-party diagnostic software.

<b>ICT ITS1</b>	Version:01	Page No.14
	Copyright: Ethiopia Federal TVET Agency	



- Conflict with devices — you should check the systems properties information available on your operating system platform, for any messages or indications of conflict.
- Device driver is faulty — try to isolate the problem occurrence to when a particular device is in use, such as a scanner or printer. A driver update may be a solution.

### **Some poorly designed programs do not behave in a civilized fashion**

In other words, programs may take control and not yield to other programs when they need processor time. On some operating systems it is possible to view the activity of applications or processes. In *Microsoft Windows XP/2000* you can press the Ctrl + Alt + Delete keys and access the Task Manager. From there you can attempt to kill any process that is consuming more than its fair share of processor time.

### **The operating system has generally become unstable**

The most reliable solution is to reinstall the operating system. Alternatively you may be able to restore to a backup of the system, where performance levels were known to be good.

### **Typical faultfinding procedures**

#### **Flowcharts**

Fault finding procedures can be presented in several ways. For instance you could produce sets of flowcharts that consider various options based on Yes/No responses. This technique is useful for training, or use of, first line helpdesk staff in responding to caller's difficulties. The downside to using flowcharts is that a different flowchart would be needed for every possible problem, which would be very time-consuming to produce and not something that a field technician is likely to carry around. Nevertheless they can be a useful tool.

#### **Communicate**

For more experienced technical support staff, sometimes a few pointed questions, to the user of the system, may be able to isolate the cause of a problem quickly. The approach when talking to the user may be to establish a history. Establish a history means to find out what worked before, what changed, and what works now. The solution might be simple – change it back.

#### **Read and respond**

<b>ICT ITS1</b>	Version:01	Page No.15
	Copyright: Ethiopia Federal TVET Agency	



Make sure you read carefully any error messages. When programmers write programs they usually assign some error code to each possible error that they may expect the program to encounter. If an error message quotes a number, then write it down and check it with the manufacturer or developer. If they know the specific error code then they will be in a position to offer specific and more reliable advice. Try a workaround. For instance if you read an error message stating that there was 'No boot device found', then provide a different boot device. This could be as simple as using another bootable floppy disk, hard disk or even CD-ROM disk. If the system starts up, then you will be in a position to effect repairs.

### **KISS principle**

Keep It Simple Stupid (KISS), while sounding strange, is an approach that can be surprisingly effective. Look for the simple things first. For instance:

- If a system does not power up as you expect then consider if there is in fact power connected and turn on.
- If nothing appears on a monitor, then try a different monitor. Then you will know if the problem is the monitor or within the system unit. Another possibility is that little fingers have turned the brightness control down so that the screen simply appears black, when in fact nothing is wrong.
- If you suspect that a video card is faulty, then swap it with a known good card – if the fault continues then you know that the card is not at fault. If another card is not available then, remove the card, power the system and you should hear an appropriate audible error – no beeps and the motherboard is the likely faulty component.
- If the mouse-pointer movement seems erratic, then turn the mouse over and clean the rollers, if it still is not working properly then replace it with a new mouse. The cost of some devices is so low, in comparison to the time wasted, that it is just not worth the bother.

### **Diagnostic tools**

The most useful diagnostic tool that can be used is your brain. The tool should be used in conjunction with the KISS principle. While that is suitable for some obvious problems, there are times when more specific information is needed in order to take the appropriate corrective measures. To get good information about a systems condition, good diagnostic tools are required.

### **A POST card**

<b>ICT ITS1</b>	Version:01	Page No.16
	Copyright: Ethiopia Federal TVET Agency	



Where a system does not boot, or appears to be dead, there are some specialist interface cards that can be used to diagnose the problem. A set of LEDs (light emitting diodes) display a code that can be referenced from the manual. Example of this type of card would be:

- *Post-Probe* by Micro2000 ([www.micro2000.com](http://www.micro2000.com)).
- *ISA/PCI PC Analyzer Diagnostic Card* by Pro Tech Diagnostics ([www.protechdiagnostics.com](http://www.protechdiagnostics.com)).

### **Diagnostic software**

Where a computer is capable of starting to the boot level, you can use diagnostic software in an attempt to isolate the cause of a problem. While there is software that runs on your existing operating system (like Norton's Utilities), the better software will have its own operating system.

When a program requests access to any hardware device, it should be accessing it through the operating system and any drivers. The problem with this approach is that the operating system shields the higher-level programs from the lower-level hardware functions. If a program were to access the hardware directly, then it is highly likely that the operating system will not respond well and the system could easily crash.

If diagnostic software is operated on its own specially designed operating system, then direct access (via the BIOS) to the hardware will likely yield accurate and thorough details. Having unimpeded access to the low-level functions of the hardware means the diagnostic software is able to run rigorous testing and reporting. After all, it's unlikely that rigorous memory testing could be performed while there are several other programs currently running in memory.

Examples of good diagnostic software are:

- *Micro-Scope Diagnostic Suite* from Micro2000 ([www.micro2000.com](http://www.micro2000.com))
- *PC Certify Lite* from Pro Tech Diagnostics ([www.protechdiagnostics.com](http://www.protechdiagnostics.com))

### **Use built-in tools**

All operating systems come with utilities that are used for general checking, repair and reporting of faults. Each operating system is different but they do have some tools in common. Tools such as hard disk scanning, such as *Scandisk* from Microsoft, *fsck* (file system check) on Unix clones like Linux, and Apple's *Disk First Aid*.

If your operating system supports it, then checking the device interrupts and input/output addresses can locate problems associated with hardware conflicts, or apparent inoperative hardware. For instance you

<b>ICT ITS1</b>	Version:01	Page No.17
	Copyright: Ethiopia Federal TVET Agency	



may have a sound card installed in a system but have difficulty in getting the device to produce any sound, when you know the device is not faulty.

An example of a Device Manager can be seen using Microsoft Windows XP/2000. Right-click the *My Computer* icon, select *Properties*, then click the *Hardware* tab, then click the *Device Manager* button. If any items listed have some problem, a yellow symbol with an exclamation (!) is displayed.

### **Check for conflicting devices**

When a device (a sound card, mouse, NIC etc.) requires attention from the processor (CPU), it generates an Interrupt Request commonly known as an IRQ. It is the equivalent to a child putting their hand in the air in a classroom, because the teacher's attention is required for some reason.

There are a set number of interrupts that are available (traditionally just 0-15), for use in the typical personal computer, so it is possible for two or more devices to generate an interrupt using the same IRQ number. This is fine, provided only one device uses that request at any given time. But if a request, say IRQ 7, is generated by two devices simultaneously, then the processor will not be able to distinguish which device is in need of attention. Therefore a conflict occurs.

Each hardware device also has a base address (or IO address) where data is sent or retrieved (input or output). It's the equivalent of Post Office Boxes, all numbered and where each relates to only one person's mail. Two people can use the same PO Box, so if two devices share the same address then a conflict occurs.

Fortunately, many of the hardware conflicts of the past are significantly reduced through the use of USB connections. The USB (Universal Serial Bus) controls which device is generating an interrupt and the address of each device.

### **Swap devices**

In troubleshooting hardware problems with a personal computer, you will need to swap devices ie you replace a suspect component with a known good component. While different devices may be fitted in different ways, the basic steps remain the same. For example, while different types of RAM may be inserted differently — some may have to be inserted at an angle, others pushed directly down — the steps in removing the covers and replacing the component remain the same.

Here is a set of steps for the removal and replacement of the system unit covers:

### **Warnings**

<b>ICT ITS1</b>	Version:01	Page No.18
	Copyright: Ethiopia Federal TVET Agency	



If the case is on a retail or brand-name system that is under warranty, be very sure that opening the case will not void your warranty. Some vendors have this policy, and you may see stickers on the case that say that if they are removed or broken the warranty is void. Some have the policy without the stickers.

Case and system manufacturers are quite creative, so not every imaginable case design is covered here. If you read all of the different choices you are likely to find one that is close to what you have.

Be careful not to touch any of the internal components when removing the cover.

### **Cover removal procedure**

#### ***Disconnect cables***

Make sure the system itself is off. Detach all the cables from the back of the system case. Make a note of what went where so that you will know how to reconnect them later on.

#### ***Remove monitor and other devices***

If you have a desktop case, you of course need to move the monitor so that you can open the case. Also remove any other devices from the top of the case.

#### ***Loosen and remove cover***

The instructions for removing the cover depend on what sort of case you have. Find the one that best describes your system:

*Conventional tower:* This is the classic design that has been around for years and is still being sold. Locate the screws along the edge of the back of the case, and remove them using a screwdriver. There are usually four to six. Gently pull back on the U-shaped top cover about a half-inch.; you may have to rock it slightly. Lift the cover up off the frame of the case. Be careful, as these covers are large and unwieldy.

*Conventional desktop:* The conventional desktop case has been around since the original IBM PC in 1982, and is still sometimes seen in new systems. Locate the screws along the edge of the back of the case, and remove them with a screwdriver. There are usually five but may be fewer. Gently push the cover forward. Watch out for drive faceplates that may become caught on the cover as you try to slide it forward. On some cases, the front cover slides all the way off the front of the case. On others it will slide forward a couple of inches and stop, and then you lift it up off the case.

<b>ICT ITS1</b>	Version:01	Page No.19
	Copyright: Ethiopia Federal TVET Agency	



**Slimline Desktop:** An odd design found on some proprietary systems, the low-profile case has the screws that hold the cover on the front or rear of the case. Others may in fact be screwdriver-less, using finger tight screws. Look at the front of the case near the bottom, or the centre top at the rear. Loosen the screw(s), and slide the cover forward off the case. Watch out for drive faceplates that may become caught on the cover as you slide it.

### ***Store screws in safe place***

If you forget this step you might regret it later on.

**Remember to wear an anti-static wrist strap before touching any internal components.**

### ***Post change, re-assembly procedure***

After changing any component, you should take the following basic reassembly procedure.

### ***Power inspection***

Verify the following key items related to the system power:

- If the system case has a dual voltage switch, make sure it is set to the correct voltage eg 230/240V.
- Make sure the power switch is off. You don't want the system booting up as soon as you connect the power cord.
- If you are working in an ATX system, double-check that you have connected the power switch to the motherboard properly.
- Make sure all your drives have a power connector attached to them correctly.
- Make sure that the CPU fan and any additional case fans have their power connectors attached.

### ***Cable inspection***

- Check the cable connections to make sure they are correct.
- Check for loose connections or cables that are misaligned. Make sure the red edge of the cable is lined up to pin 1 of each device
- Check the IDE cable(s) going to the hard disk drive and CD-ROM drive.
- Check the floppy cable going to the floppy disk drive.
- Check the cables that attach the I/O port connectors and PS/2 mouse port connector to the motherboard. Most new motherboards have all these connections integrated on the motherboard, so this is not an issue.

<b>ICT ITS1</b>	Version:01	Page No.20
	Copyright: Ethiopia Federal TVET Agency	





- Make sure the cables running to the case switches and LEDs are correct. For instance, if the speaker is not connected you will not be able to hear any audible error beeps, or power good signal.

### ***Motherboard inspection***

Double-check these configuration and installation aspects relevant to the motherboard:

- Make sure the memory is inserted into the correct socket(s) and is fully seated.
- Make sure the processor is inserted correctly and is all the way into its socket.
- Ensure that the heat sink is secured properly to the processor.
- Make sure the video card is seated properly in its slot. Some motherboards, particularly proprietary ones, will also have the video fully integrated on the motherboard, so this is not necessary.

### ***Physical interference inspection***

Check the following physical issues:

- Ensure that all the drives are properly secured in their bays.
- Make sure there are no loose wires in the case that may interfere with any moving objects like the CPU fan. Some video cards can also have a fan attached and some cases can have more than one fan.

**Experience shows that it is quicker, and less frustrating, to test the operation of the system before putting the covers back on.**

### **Update drivers**

A driver is a program that is designed to operate a particular device at its lowest hardware level. The benefit of having device drivers is that any application need not know the finer details of how a device works, simply know how to ask it to do whatever it does. For example, to print a graphic on a page, a word processor need only provide the graphic to the driver and issue some command .

Drivers are usually supplied by the manufacturer of the device. While many drivers (for a wide range of devices) are included with an operating system, they are originally provided by the manufacturer. As problems are identified by manufacturers (possibly as a result of customer complaints), they will update their drivers to fix the problem. It stands to reason then, that if you have device that is experiencing some problem, that obtaining the updated driver from the manufacturer might rectify the problem. Further, it's

<b>ICT ITS1</b>	Version:01	Page No.21
	Copyright: Ethiopia Federal TVET Agency	



not necessary to wait for a known problem to manifest itself before you choose to update the driver – it's called a preventative measure.

Not all drivers are simply software added or updated on the operating system. Some devices (including motherboards, modems etc.) can have their ROM BIOS updated through using Flash Memory technology. The term flash memory is applied to special EEPROM (Electrically Erasable Programmable Read Only Memory) hardware chips. By running a program provided by the manufacturer the latest bug fixes or new protocols etc. can be applied.

However, there is a word of warning in flashing a BIOS. Some manufacturers take little care in checking if the existing BIOS to be updated is of a suitable type and/or model, and possibly provide no option to undo what is done. Flashing a BIOS is not for the faint-hearted as some errors could lead to the device being totally unusable. So it is important to make sure you get the right update!

<b>ICT ITS1</b>	Version:01	Page No.22
	Copyright: Ethiopia Federal TVET Agency	



## **Warranties**

After you have identified a faulty device, you will then have to make the decision to repair, or replace. Realistically, most electronic components are rarely repaired. The cost of finding faulty transistors, diodes, fuses, etc. is a specialist task and is high enough to make it cheaper and faster simply to replace the component. This would be true for items such as video cards, network cards, floppy disk drives, motherboards, etc.

However, there are some peripherals that are likely candidates for repair. For example, a CRT monitor that displays a blurred or dull image can be easily adjusted, as there are brightness and focus adjustments inside the cover. Refocusing a monitor is a 10 minute job for a suitably trained person. Some printers may simply need a print-head or roller replaced, so once again there no need to discard the device as unserviceable. These types of repairs should be carried out by qualified technicians and usually at a specialist repair/service centre.

If a piece of hardware is to be repaired or replaced, then the question of warranty arises. If there is no warranty exists (unlikely), or warranty has expired then perhaps the hardware can be considered as having reached its useful life, and be replaced or upgraded with one that is covered by warranty. The cost of repairs not performed under warranty can often easily justify taking this view.

Even if repairs are to be done under some warranty system then, you might want to consider some of these factors:

### **Turnaround time**

There will be a turn around time for the repairs from the time you make the call.

### **Costs**

You may be required to pay extra costs such as freight to and from the repair centre.

### **Location**

The equipment may have to be sent quite some distance to the nearest repair centre.

### **Loaners**

If a repair will take days or weeks, determine if it is possible to provide an alternative device as a stopgap measure. The last thing you want is significant downtime.

<b>ICT ITS1</b>	Version:01	Page No.23
	Copyright: Ethiopia Federal TVET Agency	



Ideally you want an arrangement where you simply make a phone call, the support people come to your premises and replace any faulty components. What you really need in a productive and busy environment is a good **Service Level Agreement**.

### **Getting support to work for you**

In business you often can't afford to be unproductive. Imagine a retail outlet with a line of customers and the 'computer is down and won't be working for two days'. How much would be lost through lost sales and disgruntled customers? It could be very expensive indeed. When you view the situation from an economical point of view, the seemingly expensive option of on-site 24/7 support services may not seem quite so expensive.

In a less system-critical environment you would still become reliant on good support services, but your needs may only extend from 9-5pm, five days a week. So choosing the support level you need is one aim of a good Service Level Agreement.

A Service Level Agreement (SLA) is a contract between a service provider and the end-user which stipulates and commits the provider to a required level of service. An SLA should contain:

- a specified level of service
- the support options
- the enforcement or penalty provisions for services not provided
- a guaranteed level of system performance in terms of downtime or uptime
- a specified level of customer support
- what software and/or hardware will be supported
- the fees and charges involved.

A poorly chosen SLA might find that you have on-site support in principle only. For instance, your agreement might be for a technician to go on-site. But after making a call the technician arrives, and the equipment is taken and sent away for repairs. The repairs or replacement might take weeks, with no other equipment acting as a temporary workaround. You may be unproductive during that time; clearly not a satisfactory situation.

Even with a well-chosen SLA you can still assist the support processes when you log a call by:

- Performing some initial troubleshooting on the equipment in an attempt to pinpoint the device at fault. In the process you will likely also determine what the cause IS NOT.

<b>ICT ITS1</b>	Version:01	Page No.24
	Copyright: Ethiopia Federal TVET Agency	



- Explaining clearly to the first-line support person (whether by phone or email), that you have isolated the cause of the problem, and what the cause is (or is not).
- Trying a few options or suggestions provided to further narrow down or solve the problem.
- Making sure you get a Call, Job or Request Number or Reference. This number will be vital in being able to track the progress of any work or equipment related to the fault.
- Being polite! Think about what it must be like being the person at the other end of the phone that clients constantly complain too.

**Escalating** is the term applied to passing the problem onto the next level of support. If the fault cannot be initially corrected, then it is passed to a more experienced and technically savvy person or team. Once again if you have the *request number*, you will be able to track progress more quickly.

Self Check 5

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. List type of boot device option ?
2. Write solution Failure to read hard disk drive?
3. Write solution CD-ROM or DVD-ROM drive not reading disks?



**Note: Satisfactory rating – 2 points**

**Unsatisfactory - below 2 points**

You can ask your teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

**List of Reference Materials**

**1. BOOKS**

2. <https://training.gov.au/Training/Details/ICTSAS506>

3. [web1.keira-h.schools.nsw.edu.au/faculties/IT](http://web1.keira-h.schools.nsw.edu.au/faculties/IT)

<b>ICT ITS1</b>	Version:01	Page No.26
	Copyright: Ethiopia Federal TVET Agency	



### 6.1. SYSTEM RESOURCES (IRQ, DMA and I/O ADDRESSES)

System resources are what allocate and setup your hardware components helping preventing hardware to work without causing issues with other hardware within your computer. System resources are setup by one or more of the following:

- Interrupt Request (IRQ)
- Input/output (I/O)
- Direct memory access (DMA)

#### 6.1. WHAT IS IRQ?

An IRQ or Interrupt request line allows a hardware device inside of the computer a direct line to the Microprocessor and tells the Microprocessor to stop what it is doing and wait until it has further instructions. Every PC computer has a maximum of 16 IRQs and is prioritized in the computer according to the importance of the device.

#### 6.2. WHAT IS DMA?

A DMA or **Direct Memory Access** is a pathway provided by the hardware to allow the hardware direct access to the computer's memory. This feature allows devices to bypass the CPU and write their information directly to the main memory.

#### 6.3. WHAT IS I/O?

An Input Output (I/O) represents the location in memory that is designated by use of various devices to exchange information amongst themselves and the rest of the PC.

### Warranties and support

Before acquiring hardware peripheral devices, it is vital to assess what kind of warranties, service and support, prospective suppliers will provide.

#### Warranties

A warranty is an agreed upon term which covers a computer or computer component. Generally, most computers have a 1 or 3 year warranty. This warranty may or may not cover the service, repair and replacement of computer parts.

ICT ITS1	Version:01	Page No.27
	Copyright: Ethiopia Federal TVET Agency	



An extended warranty is an available option provided by manufacturers or third-party companies that provides additional support and/or repair of a computer or other hardware devices beyond its standard warranty.

<b>ICT ITS1</b>	Version:01	Page No.28
	Copyright: Ethiopia Federal TVET Agency	





## Warranty

When computer hardware devices are purchased, the supplier provides a guarantee that if a fault develops in the equipment within a certain time, they will repair or replace it free of charge. Organizations need to consider the warranty conditions before purchasing to ensure their business needs will be met. Common warranty conditions include:

- The length of the warranty – typically one or more years.
- The actions needed to have the repairs undertaken. Either the repairs will be done on-site or the equipment will need to be returned to the supplier, known as return-to-base.
- How long the supplier has to make good any required repairs
- Any exclusions to the warranty, such as damage caused to hardware by accidental damage.

Many computer hardware suppliers offer extended warranties at additional cost. For example, the extended warranty may extend the period of cover from one year to three years. The level of service purchased by an organization will depend on how critical the device is to the IT system.

**A Service Level Agreement (SLA)** is an agreement which sets out the level of service and maintenance to be provided.

## Service and support

It is important to know what kind of support services are offered by the prospective supplier. There are many questions to consider such as:

- If a device requires repairs does it have to be sent back to the supplier (called 'Return to base') or will they provide on-site visits?
- What is the average response time if service is required?
- What kinds of maintenance and repair costs could be incurred during the duration of use of the device?
- Will the device require regular servicing? If so, how many services will be necessary over a one-year period?

ICT ITS1	Version:01	Page No.29
	Copyright: Ethiopia Federal TVET Agency	



Self Check 6	Written Test
--------------	--------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**II. Fill the blank space.**

- \_\_\_\_\_line allows a hardware device inside of the computer a direct line to the Microprocessor and tells the Microprocessor to stop what it is doing and wait until it has further instructions.
- \_\_\_\_\_is a pathway provided by the hardware to allow the hardware direct access to the computer's memory.
- \_\_\_\_\_is an agreement which sets out the level of service and maintenance to be provided.
- \_\_\_\_\_an agreed upon term which covers a computer or computer component.
- \_\_\_\_\_represents the location in memory that is designated by use of various devices to exchange information amongst themselves and the rest of the PC.

**Note: Satisfactory rating – 3 points**

**Unsatisfactory - below 3 points**

You can ask you teacher for the copy of the correct answers.

<b>ICT ITS1</b>	Version:01	Score =	Page No.30
	Copyright: Ethiopia Federal TVET Agency	Rating: _____	



Instruction Sheet	<b>LG28:-Hardware requirements with specified manufacturers</b>
-------------------	---

This learning guide is developed to provide you the necessary information regarding the Following content coverage and topics –

- Determining and applying suitable environmental conditions
- Considering orientation and proper functioning of different computer platforms
- Determining and applying System protection devices
- Determining and applying requirements when moving hardware
- Determining and applying suitable storage principle
- Considering and applying business requirements
- Considering OHS standards and environmental concerns

This guide will also assist you to attain the learning outcome stated in the cover page.

Specifically, upon completion of this Learning Guide, you will be able to –

- Suitable environmental conditions are determined and applied for hardware and peripherals
- General orientation and proper functioning of different computer platforms are considered in locating computer



- System protection devices are determined and applied to keep hardware form damage.
- Requirements are determined and applied when moving hardware.
- Suitable storage principles are determined and applied for hardware and associated peripherals and media.
- Business requirements are considered and applied in respect of hardware location
- Functions of computer hardware and associated OHS standards and environmental concerns are considered

### **Learning Instructions:**

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 6.
3. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3, Sheet 4 , Sheet 5, Sheet 6 and Sheet 7 ” **in page 1,8 ,15, 18,27,31 and 36** respectively.
4. Accomplish the “Self-check 1, Self-check 2, Self-check 3, Self-check 4 , Self-check 5, Self-check 6 and Self-check 7” **in page 5, 11, 17,26 30,35 and 40** respectively

<b>ICT ITS1</b>	Version:01	Page No.1
	Copyright: Ethiopia Federal TVET Agency	



Information Sheet – 1	Determining and applying suitable environmental conditions
-----------------------	--

## 1.1. Environmental conditions

Just like the environmental conditions affect us as humans, computer equipment can also be affected. In order to install and maintain equipment to gain the maximum useful life, the environmental conditions need to be considered — factors such as temperature extremes, humidity, dust, electromagnetic interference (EMI), and so on. The following notes are a discussion of these factors.

### 1.1.1. Temperature

One of the single most important factors in prolonging the life of your computer hardware is the temperature of the components. Components that run hot, have a much shorter life than those that stay cool most of the time. To keep components cool you could use cooling equipment or ensure certain procedures or actions (discussed later). A more general approach is to provide a room environment that is appropriate for the hardware.

A rule of thumb for room temperature is that computers like the temperatures that most people like. That is temperatures between 15 and 24 degrees Celsius. Having computer equipment operating in a hot room that is over 25 degrees Celsius will make general cooling equipment, such as fans, fairly ineffectual.

Some businesses have their air-conditioners on a timer that will shut off at night. In this situation you might want to make sure that computer equipment is switched off overnight, or that a special computer room is designated with independent controls.

Obviously most computer hardware can tolerate being at more extreme temperatures when they are not running. If you are transporting equipment or storing it, the temperature concerns are far less than if the equipment is actually in use. However, if you have equipment that has been exposed to very low temperatures and is then immediately turned on, you risk permanently damaging the equipment. It is essential

ICT ITS1	Version:01	Page No.2
	Copyright: Ethiopia Federal TVET Agency	



that very cold equipment be brought up to room temperature slowly before use. This is called acclimation.

When receiving new equipment during very cold weather, it is worth considering that the equipment has been sitting in very cold warehouses or trucks. You may be risking permanent damage if you switch power up the equipment while still very cold. Of particular concern are monitors, hard disks, motherboards, and chips of all kinds (processor, memory, etc.) This covers most of the computer of course.

Thermal stress is a leading cause of premature failure of electronics components. This is bad enough when the components are raised from 20 degrees to 60, but when they are raised from 0 to 60 it is much worse.

Condensation can be even more destructive. Think about how moisture condensates on a cold bottle, on a warm day, when you take it out of the fridge (usually around 5 degrees Celsius). It is quite possible for this to happen with electronic equipment as well. This does not need to cause any problems, so long as you give the condensation enough time to evaporate. If your hard disk platters have moisture on them when you spin them up, you risk destroying the drive.

The colder the equipment is, the longer it needs to sit to ensure that it comes up to a reasonable temperature before turning it on. In temperatures down 5 degrees, then you might want to wait up to 12 hours. If the device has been allowed to go to below-freezing temperatures, then wait 24 hours for the device to acclimate before plugging in the power. A more humid environment will make condensation more of a problem.

### 1.1.2. Humidity

As with temperature, computers prefer moderate humidity as opposed to either extreme. While computer equipment is not as sensitive to humidity as temperature, they can still be affected by it.

Obviously, computers are best kept dry. That means keeping it away from places or things that can get it wet. Consider the inappropriate positioning near a window if it is frequently opened, and be wary of beverages placed near the computer that could spill on it and short it out.

<b>ICT ITS1</b>	Version:01	Page No.3
	Copyright: Ethiopia Federal TVET Agency	



Using computer equipment in a humid area can be problematic, if the climate is extremely humid. Using a computer in a tropical rainforest is an example of extreme humidity. Humidity leads to corrosion and possible condensation risk, which can damage equipment. It also makes cooling the computer more difficult.

Conversely, air that is too dry can cause problems in two different ways. First, it increases the amount of static electricity that is in the room, increasing the chances of a discharge. Second, it can cause faster wear on some components that dry out over time. This includes some types of capacitors, as well as rubber rollers on laser printers.

<b>ICT ITS1</b>	Version:01	Page No.4
	Copyright: Ethiopia Federal TVET Agency	



### 1.1.3. Dirty environments

Computers operate best when they are used in a clean environment, and when they are cleaned regularly. Most offices and homes are clean enough that a computer requires no special treatment other than regular cleaning as part of routine preventive maintenance. Industrial environments however can be quite destructive on computer equipment.

Computer systems that are going to be used in dirty environments should be protected or cleaned often. Cleaning would also mean taking the covers off and cleaning the inside. If you get the chance to see the inside of a system unit that has been in an industrial environment, you will be amazed how much dirt accumulates.

One easy preventive measure is to use an air cleaner in the room where the computer is located. There are also special cases and enclosures for computer hardware designed for industrial environments to safeguard against damage due to dirt. The typical office owner only has to remember to clean their equipment occasionally and no problems will generally result

Now this might be stating the obvious, but cigarette smoke is bad. The simple fact is that cigarette smoke, especially in high concentration, contaminates and damages computer equipment. The smoke particles are very small and work their way into all sorts of places that they do not belong. The most common problems relate to storage devices. The very fine particles accumulate on read/write heads and the storage media, such as floppy disks.

### 1.1.4. Electromagnetic interference (EMI)

Probably everyone at some stage has had a radio on when there is an approaching thunderstorm. You would clearly hear the crackling and noise distortion coming from the radio. That crackling is the result of electromagnetic interference, often referred to as EMI.

All electronic devices give off electromagnetic emissions. This is radiation that is a by-product of electrical or magnetic activity. Unfortunately, the emissions from one device can interfere with other devices, causing potential problems. Just like the

<b>ICT ITS1</b>	Version:01	Page No.5
	Copyright: Ethiopia Federal TVET Agency	





crackling on the radio, interference can lead to data loss, picture quality degradation on monitors, and other problems with your PC, television set or other devices.

EMI emissions are a two-way problem; emitted by the computer system, and EMI received by the computer system. PCs generally do not cause very much interference with other devices. As with many other electronic devices, they should be certified as Class B compliant with the Federal Communications Commission (FCC). This certification shows that the PC conforms to standards that limit the amount of EMI that a PC can produce. As metals absorb EMI, you have to keep the metal covers on the computer.

PCs can be affected by electromagnetic interference from other devices, in two major ways. One is direct effects through proximity with other devices; another is electrical interference over the power lines.

Try this quick test:

- 1 Hold a mobile phone near next to an operating monitor
- 2 Send an SMS message to someone you know.
- 3 Watch the effects on picture quality.

While a more colourful test would be to place a strong magnet next to a monitor, it is not recommended as sometimes the effects can be long-lasting. Degauss is the process that demagnetises the metal components in the cathode ray tube (CRT), eliminating image distortion that can result from magnetic charges acquired by the components. Some new monitors degauss automatically whenever you turn on your monitor.

Most PCs generally do not have many problems with EMI, but for those that do, there are things that you can do to reduce EMI:

- **Physical isolation:** Devices that emit electromagnetic radiation should be kept a reasonable distance from your computers, peripherals and media. This includes television sets, radios, lights, kitchen appliances, and stereo speakers. Speakers designed for use with PCs are generally shielded and are much less of a problem.

ICT ITS1	Version:01	Page No.6
	Copyright: Ethiopia Federal TVET Agency	



- **Use dedicated circuits:** Some office buildings have separate power circuits that are intended for use by computer equipment. Keeping your computer on a circuit that is separate from the circuit running your refrigerator, arc welder, air conditioning unit etc., means that there will be much less interference passing to the computer from the other devices. The added benefit is this will also improve the quality of the power being sent to your machine in general.
- **Power conditioning:** The use of a line conditioner or uninterruptible power supply can filter out interference caused by other devices that share a line with your computer.

<b>ICT ITS1</b>	Version:01	Page No.7
	Copyright: Ethiopia Federal TVET Agency	



Self Check 1

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. List Environmental conditions affect?
2. List things that you can do to reduce EMI?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_



## 2.1. Determine any requirements as specified by the hardware manufacturer

If the manufacturer produces substances that may be deemed hazardous, then additional obligations apply. There are documents known as Material Safety Data Sheets or MSDS. A MSDS should be prepared by the manufacturer and include information on the recommended use of a substance, its physical and chemical properties, relevant health hazard information and information concerning the precautions to be followed in relation to the safe use and handling of the substance.

In a more general context, with virtually all equipment produced, the manufacturer is required to provide relevant safety information. This information is often provided as part of the user instruction/manual for safe operation. The following is a typical set of Safety Instructions for a combined Printer/Scanner/Copier.

### Example: Safety instructions

Read all of the instructions on this section when setting up and using the product.

### When choosing a place for the product

- Avoid places subject to rapid changes in temperature and humidity. Also, keep the product away from direct sunlight strong light and heat sources.
- Avoid places subject to dust, shocks and vibrations
- Leave enough room around the product to allow for sufficient ventilation.
- Place the product near a wall outlet where the plug can be easily unplugged.
- Place the product on a flat, stable surface that extends beyond this product base in all directions. If you place the product near the wall, leave more than 10cm between the back of the product and the wall. The product will not operate properly if it is tilted at an angle.
- When storing or transporting the product, do not tilt it, stand it on its side, or turn it upside down; otherwise, ink may leak from the cartridge.



- Leave more than 22cm between the base of the product and the edge of the surface on which it is placed; otherwise, the product may fall if tipped forward possibly causing injury.

### **When choosing a power source**

- Use only the type of power source indicated on the label on the back of the product.
- Be sure your AC power cord meets the relevant local safety standards.
- Do not use a damaged or frayed power cord.
- If you use an extension cord with the product, make sure that the total ampere rating of the devices plugged into the extension cord does not exceed the cord's ampere rating. Also, make sure that the total ampere rating of all devices plugged into the wall outlet does not exceed the wall outlet's ampere rating.

### **When handling ink cartridges**

- Do not open the ink cartridge packages until just before you install them.
- Do not shake used ink cartridges; this can cause leakage.
- Keep ink cartridges out of the reach of children. Do not allow children to drink from or otherwise handle the cartridges.
- Be careful when you handle used ink cartridges as there may be some ink remaining around the ink supply port. If ink gets on your skin, wash the area thoroughly with soap and water. If ink gets into your eyes, flush them immediately with water. If discomfort or vision problems remain after a thorough flushing, see a doctor immediately.
- Do not touch the circuitry that is located on the back of the cartridge.
- Do not remove or tear the label on the cartridge; this can cause leakage.
- Store each ink cartridge so that the bottom of its packaging faces down.

### **When using the product**

- Do not put your hand inside the product or touch the ink cartridges during printing.
- Do not block or cover the openings on the product.
- Do not attempt to service the product yourself.

Unplug the product and refer servicing to qualified service personnel under the following conditions:

<b>ICT ITS1</b>	Version:01	Page No.10
	Copyright: Ethiopia Federal TVET Agency	



- The power cord or plug is damaged.
- Liquid has entered the product.
- The product has been dropped or the cover damaged.
- The product does not operate normally or exhibits a distinct change in performance.

Do not insert objects into the slots on the product.

Take care not to spill liquid on the product.

Leave the ink cartridges installed. Removing the cartridges can dehydrated the print head and may prevent the product from printing.

### **If the product has a LCD panel**

Use only a dry, soft cloth to clean the display. Do not use liquid or chemical cleansers.

If the display on the product is damaged, contact your dealer.

If the liquid crystal solution contained in the LCD panel leaks out and gets on your hands, wash them thoroughly with soap and water, if the liquid crystal solution gets into you eyes, flush them immediately with water, if discomfort or vision problems remain after a though flushing, see a doctor immediately.

Before installing software we often need to know if a computer meets that software's minimum hardware requirements, like the [type of processor](#), the [amount of physical memory](#), the [screen resolution](#) or (not really a hardware issue pur sang) [available harddisk space](#).

#### **I. Processor**

The processor number is one of several factors, along with processor brand, specific system configurations and system-level benchmarks, to be considered when choosing the right processor for your computing needs.

A higher number within a processor class or family generally indicates more features, but it may be more of one and less of another. Once you decide on a specific processor brand and type, [compare processor numbers](#) to verify the processor includes the features you are looking for.

Intel's processor number system is used with the following brands:

#### **For Example**

<b>ICT ITS1</b>	Version:01	Page No.11
	Copyright: Ethiopia Federal TVET Agency	



Requirement Type	Requirement
CPU	<p>For <b>one</b> index server per TREX instance:</p> <ul style="list-style-type: none"><li><input type="checkbox"/> At least 2 CPUs</li><li><input type="checkbox"/> Recommended: 4 CPUs</li></ul> <p>With <b>two</b> index servers per TREX instance: At least 4 CPUs.</p> <p>The supported processors are listed in the TREX installation guide.</p>

## II. Physical Memory

Memory is the main component of a computer system. It stores instructions and data in binary form that is used by the central processing unit.

### For Example

Requirement Type	Requirement
RAM	At least 2 GB per CPU



### III. Disk Space

Hard-disk requirements vary, depending on the size of software installation, temporary files created and maintained while installing or running the software, and possible use of [swap space](#) (if RAM is insufficient).

A minimum base installation requires at least 15MB of disk space but you should assume that your actual disk space needs will be much larger.

For example, if you install many contributed modules and contributed themes, the actual disk space for your installation could easily be (and likely will be) larger than 60 MB (exclusive of database content, media, backups and other files which should be considered too when planning for your site).

### IV. Network Connections

Network Connections provides connectivity between your computer and the Internet, a network, or another computer. With Network Connections, you can configure settings to reach local or remote network resources or functions.

<b>ICT ITS1</b>	Version:01	Page No.13
	Copyright: Ethiopia Federal TVET Agency	





Self Check 2	Written Test
--------------	--------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. List instruction when choosing a power source?
  
  
  
  
  
  
  
  
  
  
2. List instruction when handling ink cartridges?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = _____
Rating: _____



<b>ICT ITS1</b>	Version:01	Page No.15
	Copyright: Ethiopia Federal TVET Agency	



### 3.1. Power conditioning

There are many issues with computers that are ultimately related to power problems. Providing a good, reliable power source to your computer, and peripheral, is another aspect of system care. We should take a look at how to avoid power problems, as well as energy conservation and other issues related to the use of power.

#### Typical power problems

There are a number of terms related to power and problems, some of the most common are:

- **Blackouts:** When power levels drop to virtually zero, or in other words there is NO power.
- **Brownouts:** Also called sag. A brownout occurs when power levels drop below that which is suppose to be delivered, for a sustained time. For example if you have a 230-240 volt power outlet, but the measurable level drops below 230 volts. Typically experienced in switching on of heavy equipment.
- **Surges:** Is the opposite of a brownout. It is where voltage levels increase above that which is specified at the outlet eg above 240 volts
- **Spikes:** A short sharp and very sudden increase of voltage, that also drops just as quickly eg a 240 volt supply jumps to 1000 volts or more for a period of as little as 20 milliseconds (1/50th of a second). This is typical of a lightning strike.

#### Protection from power problems

When power problems strike, they can cause permanent damage. The damage could be to your equipment or your data. The only effective way to deal with power problems is to prevent them from happening in the first place. Here are some steps you can take to greatly reduce the chances of power problems with your computer:

- **Power Control:**

ICT ITS1	Version:01	Page No.16
	Copyright: Ethiopia Federal TVET Agency	



- There are different devices that enable us to control power. Their function varies from device to device depending on what we use.

- **UPS** (Uninterruptible Power Supply):

A UPS helps in black out situations when the power is gone totally and brown outs, when voltage is low though there is power. UPS has batteries that provides back up power. When the power is gone, the battery provides voltage to the PC so that you can save your work. But it does not provide unlimited power. There are two types of UPS:

- **Standby UPS:**

SPS has a battery that begins generating power as soon as the unit detects a sag in the power supply. It takes only a split of seconds to come online. The disadvantage is that till the UPS become online, your data might get lost.

- **Online UPS:** It provides electricity to the PC all the time. It uses electricity from the AC outlet to simply recharge its batteries. When the power goes, the data is not affected because the UPS is supplying power.

- **Surge Suppressor:** Surge suppressors help to absorb power surges so that your computer does not feel their effects. They come as either separate modules or incorporated in the UPS.
- **Voltage Stabilizer:** It is a transformer that delivers relatively constant output when output voltage changes over time. The output voltage is regulated using transistor.
- **Battery:** Computer has a Chip that combines real time clock and non-volatile memory. This chip is the CMOS chip(CMOS RAM). They are designed to consume low power.
- **Generators** – where an organization requires the computer hardware to be powered for an extended length of time, a generator may be installed in addition to a UPS.

ICT ITS1	Version:01	Page No.17
	Copyright: Ethiopia Federal TVET Agency	



Self Check 3	Written Test
--------------	--------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**II. Fill the blank space.**

1. \_\_\_\_\_ when power levels drop to virtually zero, or in other words there is NO power.
2. \_\_\_\_\_ Is the opposite of a brownout. It is where voltage levels increase above that which is specified at the outlet eg above 240 volts
3. \_\_\_\_\_ A short sharp and very sudden increase of voltage, that also drops just as quickly eg a 240 volt supply jumps to 1000 volts or more for a period of as little as 20 milliseconds.
4. \_\_\_\_\_ help to absorb power surges so that your computer does not feel their effects. They come as either separate modules or incorporated in the UPS.
5. \_\_\_\_\_ Computer has a Chip that combines real time clock and non-volatile memory.

**Note: Satisfactory rating – 3 points**

**Unsatisfactory - below 3 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = _____
Rating: _____

<b>ICT ITS1</b>	Version:01	Page No.18
	Copyright: Ethiopia Federal TVET Agency	



Information Sheet – 4	Determining and applying requirements when moving hardware
-----------------------	--

#### **4.1. Determining your needs**

Before any venture into selecting any new equipment or services, it is important to have a clear understanding of your needs. If you don't fully understand your needs then it is not possible to ensure those needs are correctly met. In other words, know exactly what you want before you try to get it.

#### **4.2. Undertake a requirements analysis**

While we will not be examining all the finer details of performing a proper requirements analysis, it is worthwhile covering some of the basics.

Firstly, it is vitally important to put your goals into clear and concise terms. This might be in terms of a problem definition, or business plan for expansion, or upgrading your capabilities. Your definition should not include any details of specific solutions as far as equipment, suppliers etc.

You should also include a set of criteria such as time and cost limitations, types and levels of support, etc. If you document all these requirements, when you finally make your decision and implement it, you will be able to determine if it constitutes a successful project or not.

After considering your overall goals and criteria, you can then put into simple and uncomplicated terms what would be a solution to the problem or requirement.

#### **Evaluate your alternatives**

Collect all the information you can about the types of equipment available, the suppliers of that equipment, the training required to use the equipment or associated programs.

<b>ICT ITS1</b>	Version:01	Page No.19
	Copyright: Ethiopia Federal TVET Agency	



You need to have an open mind about the alternatives. Do not think that there is only one right choice, as there are always viable options. For example, you may not need to purchase all new equipment when a few upgrade options may be both acceptable and economical. There is always more than one option!

Once you have a comprehensive list of what is available, compare that list with any organisational guidelines and policies that are in place. Many large organisations and government departments have set criteria for purchasing equipment. It's necessary to familiarise yourself with those guidelines before making any recommendations or purchases. There may be organisation guidelines on the minimum standards required for equipment. Those standards might relate to:

- international or industry standards
- supplier restrictions, approved suppliers or other requirements
- purchasing guidelines (there may be different guidelines depending on the amount of money to be spent)
- minimum warranties and/or guarantees
- support levels required
- how often equipment should be automatically reviewed or updated etc.

### **Making recommendations**

After reviewing all the information above, you would then make recommendations, or make the purchases.

The important point to note is that if you do not have clearly in mind the equipment and services that you need, it is unlikely that you will make the best choices. In addition you may make the best choices in equipment, etc but there may be organisational reasons why your selection will not be approved.

### **Standards**

#### **Compulsory standards**

In Australia, as in the rest of the world, there are many **standards** with which equipment needs to comply. These standards may be from both International and Australian government bodies or from industry groups.

<b>ICT ITS1</b>	Version:01	Page No.20
	Copyright: Ethiopia Federal TVET Agency	



Some of the most important standards organisations are:

**International Organization for Standardizations (ISO)**

ISO is the world’s largest developer of standards. An ISO Standard can be anything from a four-page document to one several hundred pages long, and they will be increasingly available in electronic form. It carries the ISO logo and the designation ‘International Standard’. In most cases, it is published in A4 format — which is itself one of the ISO standard paper sizes.

**Australian Communication Authority (ACA)**

The Australian Communications Authority (ACA) is responsible for regulating telecommunications and radio communications, including promoting industry self-regulation and managing the radio frequency spectrum. The ACA also has significant consumer protection responsibilities.

**Standards Australia**

Standards Australia is an independent organisation, not directly associated with government, although the Commonwealth Government and State governments are listed among its members.

**Australian Electrical and Electronics Manufacturing Association (AEEMA)**

Australian Electrical and Electronics Manufacturing Association (AEEMA) is the leading industry body representing Australia’s information and communication technology (ICT), electronics and electrical manufacturing industries. AEEMA members supply infrastructure, products and manufacturing-related services to Australian and world markets.

**Federal Communications Commission (FCC)**

The Federal Communications Commission (FCC) is an independent United States government agency. The FCC is charged with regulating interstate and international communications by radio, television, wire, satellite and cable.

**Institute of Electronic and Electrical Engineers (IEEE)**

The Institute of Electronic and Electrical Engineers (IEEE) promotes the engineering process of creating, developing, integrating, sharing, and applying knowledge about electro and information technologies and sciences.

<b>ICT ITS1</b>	Version:01	Page No.21
	Copyright: Ethiopia Federal TVET Agency	





There are many more bodies that determine standards in a wide range of Information and Communication Technology (ICT) related products and services. When selecting any product, whether for domestic or commercial use, meeting the appropriate standards should be the first thing that is checked. Often compliance with the standards is easily recognised by the stickers and stamps on the products and its packaging.

### **standardization**

One of the most beneficial features about the general design of computer systems is that they are modular. While for many they seem like black boxes and the inner workings are a mystery, they are in fact made of mostly standardised components that are connected in standardised ways. This is called an open design and is generally considered to be responsible for the success of the PC (Personal Computer) platform over the last two decades.

Standardisation enables the relatively easy interoperability of different components within the computing world. It is the single most important factor that provides the choices that make the PC so flexible and accommodating. It is what makes it possible for the average person to make his or her own custom machine or to repair one that uses standard components. It's not always perfect, but it beats the alternative: a closed design, where one company or group of companies controls what hardware you can use in your system.

In order to get the real benefits of standardisation, however, one must make use of standard components and designs. Unfortunately, some PC designs abandon the open nature of standard PC designs by incorporating proprietary designs. These are systems where the PC maker has decided to use components that are not standardised, or has implemented standard components in a non-standard manner.

The designers of such systems usually have good intentions. They typically decide to make use of proprietary designs because they feel they can deliver a better product to the customer at a lower cost if they do this. Sometimes this is the case as some people like the special features of certain proprietary designs.

<b>ICT ITS1</b>	Version:01	Page No.22
	Copyright: Ethiopia Federal TVET Agency	



The problem with proprietary designs is that they aren't standard. By moving away from standardisation, proprietary designs give up the advantages of standard components. Here are some of the more important issues with such systems:

- **Choice and flexibility:** Proprietary designs are less flexible than standard ones. You usually have fewer choices in components when you buy the system, because the design will usually be based around specific choices made by the company's engineers.
- **Expandability and upgradeability:** Proprietary systems are more difficult to expand or upgrade than standard ones. If they are not designed to use standard components then you are limited in your expansion and upgrade options to whatever the manufacturer allows. This means you have fewer options, and you will also usually pay significantly more for any components you try to buy. If a new technology comes along a year after you buy your machine, you have to hope that the manufacturer will decide to support it.
- **Service:** PCs made from standardised components can be repaired by any competent PC technician, with some research and assistance. Proprietary systems must be worked on by those who have been specifically trained in how they are constructed. Again, this reduces your options and usually increases your costs.
- **Repair:** With a proprietary system you must go back to the manufacturer for any replacement parts for the system. These usually cost far more than standardised replacements, if they are available at all.
- **Comprehension:** Proprietary systems are more difficult to understand than standard ones, which matters if you want to really know what's going on. Worse, in some cases the proprietary nature of some subsystems is often not made available. As an example, standard IDE/ATA hard disk channels, found in virtually all PCs, support two devices (such as a second hard disk or CD/DVD drive). Some companies create their systems so that their IDE/ATA hard disk channels only support one device, but they don't mention this in the product manual. This leads to much frustration when

ICT ITS1	Version:01	Page No.23
	Copyright: Ethiopia Federal TVET Agency	



someone tries, for example, to add a second hard disk to that system and it doesn't work. They will usually think it is a problem with the hard disk.

It's not the case that a system is either 'standardised' or 'proprietary', there is much scope for movement along those two points in design. Some PCs are made entirely of standardised components, but proprietary machines may still use at least some standardised parts. It can be a voyage of discovery to find out what is standard and what is not in such a machine.

The most proprietary designs are the all-in-one systems that include everything in one physical case, which are sold like appliances. Be very careful of such designs, because if anything goes wrong, everything is affected. If your PC has the logic components and the monitor in the same case, what happens if the monitor fails, or you decide you want a bigger one?

As for the more specialised notebook PCs, they all should be considered proprietary. This is one of the reasons why you should only consider a notebook if the portability of these units can be justified.

### **Quality**

One of the most difficult tasks in the selection of computer components, or systems, is in determining quality. What represents a quality product? Possibly one of the most important things to about quality is that you need to define and determine it for yourself, and ignore the claims made about it.

We could attribute certain aspects to a product that help determine its quality. Attributes such as performance levels, typical failure rate during manufacture, durability, etc. What is high-quality for you depends entirely on what is important to you. Here are a few different aspects of quality to keep in mind. You have to decide which of these, if any, are important to you. And for most people, there may well be other critical issues not mentioned:

**Features:** One aspect of quality may be the features of a product compared to competing products. Most would consider a product that has significantly more capabilities than another to be superior, all else being equal. Very often it is not equal. For example, it is quite common for product X to have more features than product Y while sacrificing other quality aspects.

<b>ICT ITS1</b>	Version:01	Page No.24
	Copyright: Ethiopia Federal TVET Agency	



**Form, fit and function:** For many, quality is in part defined by the way the item looks, how its parts fit together, and its overall feel. Does it look professionally made? Do the components mesh together smoothly? Does it seem solid? This is the ‘kick the tires’ school of quality, and it definitely has some validity. These are rather subjective notions, but no less important for being a matter of personal judgment.

**Design and build:** While the capabilities of most computers are defined primarily by their constituent components, the whole is still greater than just the sum of the parts. How the unit is designed and the care with which it has been assembled can be very important. Some manufacturers may add special enhancements to their products that some people consider to improve the quality.

**Reliability:** Everyone who buys a product wants it to last a long time and work without problems. Products that break frequently or wear out quickly are of lower quality than those that last a long time and remain trouble-free. But once again it may not be that simple, as a product with more features has more potential parts to fail. It’s easier to make a highly reliable simple widget than a highly reliable complex one.

**Service:** The quality of a product is definitely affected by the quality of the company that sells and supports it.

**Quality**, like many other key attributes of any product, is an exercise in trade offs. More quality usually costs more money, whether you are talking about computers, clothes dryers, cars or anything else. Quality is also a matter of the pride of the company making the product, and that’s not strictly a matter of how much money you throw at a problem.

**Example: purchasing a ‘quality’ motherboard**

Let’s consider the example of purchasing a motherboard. The one factor in choosing a motherboard that is probably over-emphasized by most suppliers and by many high-end users is **performance**. Often the word performance is commonly interpreted as speed. But that is deceptive, as performance should not only encompass speed but stability, reliability, compatibility and other factors that are important to the individual user. A board that can run every application thrown at it and never crash may be described as a great performer by one user, but be called a poor performer by another who only wants to run a limited number of programs extremely quickly.

<b>ICT ITS1</b>	Version:01	Page No.25
	Copyright: Ethiopia Federal TVET Agency	



Most users look at the various **benchmarks** provided on the hardware-oriented websites and choose one of those that get the higher marks. Unfortunately, these comparisons focus strictly upon the speed of the motherboard, and completely ignore the other important issues such as reliability, compatibility and stability. Basically any number of motherboards using the same chipset will almost certainly be within a few percentage points of each other as far as benchmarked speed is concerned, and not noticeable to most users. Actually, benchmark results should probably be the last consideration when selecting a motherboard, not the first. While some of the hardware-oriented websites also claim to test motherboards for stability and reliability, this is very likely not the case. In order to test for either of these, the motherboard would need to be exposed to many days, or even weeks, of stress testing under various conditions. You can be certain that any reputable motherboard manufacturer has probably already done this with their prototypes, so once again we can assume that most motherboards from major manufacturers will be very close in this regard.

Hardware **compatibility** is the ability for various components from different manufacturers to seamlessly integrate, ie work together without problems. Hardware compatibility is an area that is extremely difficult to test, even for the manufacturer. The main reason for this is that the open architecture of the PC platform allows manufacturers to vary in how they implement certain standard features, to best suit their own particular needs. Because of the large number of manufacturers and components, testing every possible combination is virtually impossible. Because of this, compatibility testing will typically consist of testing those components that are determined to have a large market share. In this case, only time in the field will truly determine how compatible the motherboard is with various components. If you have the need to use a device that is not one of the most commonly used, you may wish to find out if the manufacturer has tested it already. Most vendors and manufacturers will not warranty compatibility problems unless they have specifically stated that the device in question will work.

### **Hardware compatibility list (HCL)**

One offering by Microsoft, that is of real assistance, is their **Hardware compatibility list** (HCL). A HCL is provided with most of their operating systems. In an environment where

<b>ICT ITS1</b>	Version:01	Page No.26
	Copyright: Ethiopia Federal TVET Agency	



significant investment in equipment is to be made, it is a worthwhile resource to use in product selection.

Just to complicate the issue of quality a little further, some hardware websites claim to evaluate the quality of a motherboard by looking at the components used (SIMM/DIMM slots, capacitors, etc). Using this definition, it is impossible to determine quality based upon a single motherboard, and certainly impossible by merely looking at it. It is entirely possible to design and construct a motherboard out of average quality components that has a higher quality in the finished product than one that is poorly designed or constructed using high quality materials.

Quality should be a measure of the overall percentage of equipment that meets or exceeds their stated specification. It is no coincidence that industry quality awards are given to those companies with the best **process**, not the ones that use the best materials.

<b>ICT ITS1</b>	Version:01	Page No.27
	Copyright: Ethiopia Federal TVET Agency	



Self Check 4

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. Define International Organization for Standardizations (ISO)?

2. Define Institute of Electronic and Electrical Engineers (IEEE)?

3. What is Hardware compatibility?

**Note: Satisfactory rating – 2 points**

**Unsatisfactory - below 2 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.28
	Copyright: Ethiopia Federal TVET Agency	



### 5.1. Introduction

We need to have an awareness of possible consequences of inappropriate storage of hardware, peripherals and Media. Based on the nature and characteristics of the hardware we will determine how and where to store them. Points to consider when storing hardware, peripherals and storage media including:

- Climatic effects
- OHS considerations
- OHS standards
- Ease of access.
- Workstation
- Ventilation
- electrical safety
- manual handling
- Security
- Stability
- Posture

### 5.2. Storing equipment

You will find that manufacturers will almost invariably require that equipment should be stored in the same packaging in which it was delivered. While this is valid, in principle, often it can be impractical. Empty packaging can consume significant storage space, which may seem not justifiable on a cost basis. However, if you do not have on-site support then to return equipment to the supplier, you will need enough to cover the basics. For example, if you have five printers from one manufacturer, you may choose to keep the packaging of one printer.

Just like locating equipment, when storing equipment you must consider the factors of temperature, humidity, dust etc. Although if equipment is not in use then such factors as temperature are less of an issue than if the equipment were in service ie in current use.

<b>ICT ITS1</b>	Version:01	Page No.29
	Copyright: Ethiopia Federal TVET Agency	





### 5.3. Manufacturer's requirements

When handling computer equipment, it is advisable to follow the manufacturer's guidelines on handling and storage. The most obvious place to find that information would be the User Guides/Manuals that accompany the product.

While some documentation can be difficult to find, in a cupboard full of manuals, it is also common to have no documentation for the equipment in printed form. These days, many of the manuals and manufacturer guidelines are in electronic form supplied on floppy disk or CD-ROMs.

One of the best avenues, to locate the current information, would be the Internet. If in

### 5.4. Locating equipment

Sometimes when determining the most appropriate location, there are competing interests. From a security viewpoint, it may not be advisable to locate important network servers within easy access from the general public, or even unauthorised employees. But from an accessibility viewpoint, it maybe convenient for service personnel to have easy and unsecured access to all equipment. Still, there are the physical services (such as power, phone, network communications etc.) where equipment could be placed in the most convenient and cost-saving location close to outlets and connectors.

### 5.5. Security

When locating equipment you would need to determine the priorities and adjust or compromise the competing interest accordingly. For example, if you have a network server that contains sensitive accounting and/or payroll data, you would not want general staff (meaning those that should not be handling account/payroll data) to be able to gain access. You could of course restrict access by software such as username/passwords etc., but that would not stop someone from physically taking the hard disk drive in order to steal or copy it.

<b>ICT ITS1</b>	Version:01	Page No.30
	Copyright: Ethiopia Federal TVET Agency	



Where sensitive or critically important hardware is concerned, it would be advisable to locate the equipment in a secure location, such as a lockable cupboard or room. Access can then be more traditionally controlled by security key access.

### **5.6. Accessibility**

Consider for a moment that you are a service technician where you go out on location to various businesses. You are called to fix a problem with a server or other equipment, but when you arrive you find the equipment is locked in a tiny cupboard, where the person with the key is out. When you finally gain access you find it buried under a pile of boxes and papers etc. Get the picture!

When locating equipment, take into account that from time to time someone will need to physically access it.

### **Disposing of Used Equipment**

- Various guidelines for disposing of equipment:
  - Manufacturer documentation
  - Local environmental regulators
- Danger posed by monitors and power supplies
  - Residual charge in capacitors can cause shock
  - Modern devices discharge if unplugged for 60 minutes
  - Older devices may require discharge with a probe
- Destroy secondary storage devices with sensitive data

<b>ICT ITS1</b>	Version:01	Page No.31
	Copyright: Ethiopia Federal TVET Agency	



Self Check 5	Written Test
--------------	--------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. List Points to consider when storing hardware, peripherals and storage media?
  
2. Define Disposing of Used Equipment?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.32
	Copyright: Ethiopia Federal TVET Agency	



### 6.1. Total cost of ownership

The initial purchase price of a computer hardware device is only part of the total cost of the device, over the lifetime of the device. Additional costs will include:

- costs of hardware and software upgrades
- costs of consumables. For devices such as printers, the cost of replacement print cartridges over the lifetime of the device can often be greater than the initial purchase price.
- maintenance costs
- cost of technical support
- cost of training

### 6.2. Support

Technical support is provided by manufacturers for users after the purchase of a computer hardware device. Access to this support is commonly limited to users who have registered the purchase of the product. Forms of technical support include:

- telephone support
- email support (usually with a guaranteed response time)
- access to support on internet such as:
  - frequently asked questions (FAQs)
  - troubleshooting guide
  - downloads of latest drivers and software updates

### 6.3. Compatibility

<b>ICT ITS1</b>	Version:01	Page No.33
	Copyright: Ethiopia Federal TVET Agency	



Compatibility is the ability of a system or a product to work with other systems or products without special effort on the part of the customer. One way products achieve interoperability is to comply with industry interface standards. For example, a memory module is compatible with a motherboard because the manufacturer of the memory module and the motherboard both work to the same industry standard.

#### **6.4. Technical specifications**

Once the business requirements have been considered, the technical specifications of the hardware device need to be evaluated. Areas for evaluation include the following:

- processing speed of the CPU
- storage capacity of the hard drive
- size of memory (RAM)
- software capabilities
- compatibility with existing systems
- upgradeability

The technical specifications to be considered will depend on the computer hardware device to be purchased. For example, technical specifications to be considered for a printer include:

- interface – USB or network
- resolution – measured in dots per inch
- printing speed – measured in pages per minute
- memory
- paper capacity

#### **6.5. Occupational Health and Safety (OH&S) Requirements and safe work practices**

<b>ICT ITS1</b>	Version:01	Page No.34
	Copyright: Ethiopia Federal TVET Agency	



In NSW, the OH&S legislation includes the Occupational Health and Safety Act 2000 and the Occupational Health and Safety Regulation 2001. Work cover NSW has the responsibility for administering this legislation.

Employers have a responsibility to provide a safe and healthy workplace for all employees. It also requires all workers to be aware that they have a duty to follow safe work practices to prevent injuries to themselves or other workers.

Organizations will develop procedures for safe working practices as a tool for implementing their OH&S policies and training staff.

For further information click on the following link: [Apply occupational health and safety procedures](#)

## 6.6. Manual handling

Computer hardware devices and consumables such as printer paper boxes can be very heavy and care should be taken when manually handling these objects.

Manual handling is one of the most common causes of accidents in the workplace. Workcover NSW <<link to <http://www.smartmove.nsw.gov.au> >>

defines manual handling as:

*“any activity that involves lifting, lowering, carrying, pushing, pulling, holding or restraining. It may also include stretching, bending, sustained and awkward postures, and repetitive movements.”*

Recommendations on practices to reduce the risk of manual handling injury at work include:

- hold the load close to your body
- store loads close to where they will be used
- store heavy loads near waist height
- use mechanical aids such a trolley when lifting heavy loads
- don't lift heavy loads when sitting down

ICT ITS1	Version:01	Page No.35
	Copyright: Ethiopia Federal TVET Agency	



To find the weight of a device refer to the device specifications in the user manual. Always check the manufacturer's recommendations before handling.

## 6.7. Safe electrical work practices

Computer hardware should be located close to a suitable electrical outlet. The use of long extension cords is a trip hazard. If no power outlet is available, a new fixed power outlet may need to be installed. Any fixed electrical installation is required by law to be installed by a licensed electrician.

Cables should be kept away from the floor, and a person's workspace. Cables on the floor are easily damaged by trolleys and chair castors.

Use switched power boards and not double adapters or piggy backed plugs.

Routinely inspect cables for any damage. Damaged cables should be disconnected and removed.

Testing and tagging refers to the practice of testing electrical equipment (which is designed for connection by a flexible cord), by an appropriate person. If the equipment is compliant a tag is attached which is marked with the name of the person or company who performed the test, and the test date or retest date.

Any component such as a computer power supply which has a mains (240 volt) power connection can only be opened and repaired by a qualified technician. CRT monitors can have very high electrical potential levels even after they have been switched off and must only be opened by a qualified technician.

Electrical circuits for fixed wiring are protected from overload by a circuit breaker. The circuit breaker will trip if the circuit is overloaded. If this happens, it is an indication that the number of electrical appliances on that circuit should be reduced.

<b>ICT ITS1</b>	Version:01	Page No.36
	Copyright: Ethiopia Federal TVET Agency	



Self Check 6

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. Write additional costs ownership?
2. Write technical support include?
3. List the technical specifications of the hardware device need to be evaluated?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.37
	Copyright: Ethiopia Federal TVET Agency	





### 7.1. Introduction

Regardless of the industry in which you work, there are legal requirements that insist on establishing a safe work environment. There exists an Occupational Health and Safety Act in all states of Australia. It describes the general requirements necessary to ensure a safe and healthy workplace. It is also designed to reduce the number of injuries in the workplace by imposing responsibilities on employers, employees and others.

Manufacturers of equipment will also provide health and safety information related to their products. It is advisable to review some of the typical requirements that a manufacturer may put forward.

In order to effectively promote a safe work environment, it is prudent that safe work practices be adopted. We will also take a look at how to determine safe work practices.

### 7.2. An overview of the Occupational Health and Safety Act and Regulation

The fundamental purpose of Health and Safety legislation is to:

- secure and promote the health, safety and welfare of people at work
- protect people at a place of work against risks to health and safety arising out of any activities of people at work
- promote a safe and healthy environment for people at work that protects them from injury and illness and that is adapted to their physiological and psychological needs
- provide for consultation and cooperation between employers and workers in achieving the above
- ensure that risks to health and safety at a place of work are identified, assessed and eliminated or controlled



- develop and promote community awareness of occupational health and safety issues
- provide a legislative framework that allows for progressively higher standards of occupational health and safety to take account of changes in technology and work practices
- protect people (whether or not at a place of work) against risks to health and safety arising from the use of machinery that affects public safety.

In New South Wales, the *Occupational Health and Safety Regulation 2001* is intended to support the earlier *Occupational Health and Safety Act 2000* in achieving reductions in the incidence of workplace injuries and disease. It replaced all the regulations made under the *Occupational Health and Safety Act* back in 1983 and others. Much of the legislation being replaced was outdated and overly restrictive.

This current set of regulations adopts a performance-based approach to occupational health and safety while still maintaining specific controls in highly hazardous areas. The best practice approach requires that regulatory proposals:

- have clear objectives and focus only on fixing identified problems
- regulate the ends and not the means
- minimise the number of government agencies involved
- promote certainty through clearly stated criteria for the assessment of applications for approvals, permits, licences, etc and publicly indicated timeframes for the assessment process
- are simple for users to understand
- are easy to enforce
- have a high voluntary compliance rate
- are subject to regular review
- do not restrict competition
- maximise benefits and minimise costs
- Use commercial incentives rather than command and control rules, for example by:
  - information provision

<b>ICT ITS1</b>	Version:01	Page No.39
	Copyright: Ethiopia Federal TVET Agency	



- encouraging quality assurance backed up by a statute only where necessary
- providing accessible legal remedies so that consumers, rather than government, can act to enforce their rights without prohibitive costs
- shifting risk management from government to the private insurance market.

### 7.3. Determine safe working practices

#### Training

All staff members undertaking tasks that may be hazardous should be given, or have, the appropriate experience and/or qualifications. Organisations should have recruitment procedures that should ensure that persons chosen to undertake tasks have the necessary competencies. All employees should receive training where appropriate to ensure they possess the required skills and experience to carry out their tasks safely.

Training should include the knowledge of the **Safe Work Procedures (SWP)**. Safe Work Procedures are written guidelines for all work activities that have been identified as posing some form of risk. It may include:

- Lifting and carrying
- Handling hazardous substances
- Working in confined spaces
- Use of particular equipment, eg drill, measuring device, cutting tool or even a computer.

If a serious accident or injury occurs, and the matter is taken to court, it would be wise if the employer were able to prove that the appropriate training had taken place. So upon completion of training (or an evaluation of competencies) the employee should sign a form acknowledging that they are aware of the particular safe working procedure. This can also form a safeguard for the employee, ensuring that management are fulfilling their responsibilities.

#### Risk assessment

ICT ITS1	Version:01	Page No.40
	Copyright: Ethiopia Federal TVET Agency	



One of the easiest ways to achieve safe working practices is to be prepared in advance. Being prepared means to: gain knowledge of the things that can go wrong and how to correct them. In other words there must be some form of risk assessment undertaken. The simplest and most practical form of implementing safe practices is to create **checklists** which cover the areas that need particular attention. By using a checklist you will avoid oversight and possible legal ramifications in the event of serious injury to a person, or damage to expensive equipment.

The more questions, and the more specific the question, the more likely that all risks will be identified. If a risk is not identified, then it stands to reason that preventative measures will not be taken to minimise injury. Carefully consider and compare the two checklists below for detail, clarity and ease of use.

<b>ICT ITS1</b>	Version:01	Page No.41
	Copyright: Ethiopia Federal TVET Agency	



## Manual handling checklist

	Yes	No	Comment
All manual hazards in the workplace have been documented.			
Control measures have been implemented to eliminate the risks associated with manual handling or steps taken to minimise risks.			
Adequate information, instruction, training and supervision are provided to ensure that risks from manual handling are minimised.			
Control measures have focussed on job or task redesign, so that work may be carried out without the risk or to reduce the risk of manual handling.			
Mechanical or other manual handling aids (trolleys, ramps etc) have been provided where these can reduce the risk of manual handling.			
A system is in place to: <ul style="list-style-type: none"> <li>• monitor &amp; review control measures</li> <li>• encourage employees to report activities that could present the risk of injury.</li> </ul>			
A system is in place to ensure that all accidents, incidents and near misses, injuries and ill health involving manual handling are reported, investigated and recorded, and appropriate corrective measures are implemented.			



Self Check 7	Written Test
--------------	--------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. Write the fundamental purpose of Health and Safety legislation?
  
  
  
  
  
  
  
  
  
  
2. Write Safe Work Procedures are written guidelines for all work activities that have been identified as posing some form of risk?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = _____
Rating: _____



<b>ICT ITS1</b>	Version:01	Page No.44
	Copyright: Ethiopia Federal TVET Agency	



## Instruction Sheet

## LG29: Monitor threats to the network

This learning guide is developed to provide you the necessary information regarding the Following content coverage and topics –

- Using third-party software to evaluate and report on system security
- Identifying security threats
- Ensuring carry-out spot checks and other security strategies
- Investigating and implementing inbuilt or additional encryption facilities
- Preparing and presenting an audit report and recommendation
- Obtaining approval for recommended changes

This guide will also assist you to attain the learning outcome stated in the cover page.

Specifically, upon completion of this Learning Guide, you will be able to –

- Use third-party software or utilities to evaluate and report on system security
- Review logs and audit reports to identify security threats
- Carry-out spot checks and other security strategies to ensure that procedures are being followed
- Investigate and implement inbuilt or additional encryption facilities
- Prepare and present an audit report and recommendations to appropriate person
- Obtain approval for recommended changes to be made

### Learning Instructions:

5. Read the specific objectives of this Learning Guide.
6. Follow the instructions described below 3 to 4.
7. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3, Sheet 4, Sheet 5 and Sheet 6” in **page 1, 4, 10,14, 20,and 23** respectively.

<b>ICT ITS1</b>	Version:01	Page No.45
	Copyright: Ethiopia Federal TVET Agency	





8. Accomplish the “Self-check 1, Self-check t 2, Self-check 3 , Self-check 4, Self-check 5 and Self-check 6” in **page 3, 9, 13, 19,22,and 25** respectively

<b>ICT ITS1</b>	Version:01	Page No.46
	Copyright: Ethiopia Federal TVET Agency	



## 1.1. Introduction

**Computer network** : is a system in which computers are connected to share information and resources. The connection can be done as peer-to-peer or client/server or LAN or WAN.

The term network monitoring describes the use of a system that constantly monitors a **computer network** for slow or failing components and that notifies the **network administrator** (via email, pager or other alarms) in case of outages. It is a subset of the functions involved in **network management**.

Network security consists of the **requirements** and **policies** adopted by the **network administrator** to prevent and monitor **unauthorized** access, misuse, modification, or denial of the **computer network** and network-accessible resources.

## 1.2. Network threats

Network threats are intentional activities to cause damage, misusing resources, or other aggressive action on network system.

### Some of Network threats

- Unauthorized accessing
- Misusing of resources
- Modification of network resources
- Denial of services

There are different ways to monitor threats to the network. Some of them are: -

- By using software Utilities
- By using security mechanism
- By Using encryption facilities

## 1.3. Identifying security threats

### Explain why security is important

Computer and network security help to keep data and equipment functioning and provide access only to appropriate people. Everyone in an organization should give high priority to security because everyone can be affected by a lapse in security.



Theft, loss, network intrusion, and physical damage are some of the ways a network or computer can be harmed. Damage or loss of equipment can mean a loss of productivity. Repairing and replacing equipment can cost the company time and money. Unauthorized use of a network can expose confidential information and reduce network resources.

#### 1.4. Describe security threats

To successfully protect computers and the network, a technician must understand both types of threats to computer security:

- Physical – Events or attacks that steal, damage, or destroy equipment, such as servers, switches, and wiring
- Data – Events or attacks that remove, corrupt, deny access, allow access, or steal information

Threats to security can come from the inside or outside of an organization, and the level of potential damage can vary greatly:

- Internal – Employees have access to data, equipment, and the network
  - Malicious threats are when an employee intends to cause damage.
  - Accidental threats are when the user damages data or equipment unintentionally.
- External – Users outside of an organization that do not have authorized access to the network or resources
  - Unstructured – Attackers use available resources, such as passwords or scripts, to gain access and run programs designed to vandalize
  - Structured – Attackers use code to access operating systems and software

<b>ICT ITS1</b>	Version:01	Page No.48
	Copyright: Ethiopia Federal TVET Agency	



Physical loss or damage to equipment can be expensive, and data loss can be detrimental to your business and reputation. Threats against data are constantly changing as attackers find new ways to gain entry and commit their crimes.

<b>ICT ITS1</b>	Version:01	Page No.49
	Copyright: Ethiopia Federal TVET Agency	



Self Check 1	Choose Test
--------------	-------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. choose the best answer from the following question**

\_\_\_\_\_ 1. \_\_\_\_\_ is a system in which computers are connected to share information and resources

- A/Network threat    B/Network Security    C/Computer Network    D/Protocol

\_\_\_\_\_ 2. Which one is not Network threats are intentional activities to cause damage, misusing

resources, or other aggressive action on network system.

- A/Unauthorized accessing    B/ Misusing of resources    C/Denial of services    D/All

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = _____
Rating: _____

<b>ICT ITS1</b>	Version:01	Page No.50
	Copyright: Ethiopia Federal TVET Agency	



## 2.1. Introduction

**Computer Security:** The prevention and protection of (computer) assets from unauthorized access, use, alteration, degradation, destruction, and other threats.

**Network security** involves the authorization of access to data in a network which is controlled by the network administrator and the organization policies. Users choose or an ID and password or authenticating information that allows them access to information and program within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done.

**Privacy:** The right of the individual to be protected against interruption into his personal life or affairs, or those of his family, by direct physical means or by publication of information.

**Security/Privacy Threat:** Any person, act, or object that poses a danger to computer security/privacy.

## 2.2. Computer Security and Privacy/Vulnerabilities

- Physical vulnerabilities (Eg. Buildings)
- Natural vulnerabilities (Eg. Earthquake)
- Hardware and Software vulnerabilities (Eg. Failures)
- Media vulnerabilities (Eg. Disks can be stolen)
- Communication vulnerabilities (Eg. Wires can be tapped)
- Human vulnerabilities (Eg. Insiders)

With an increasing amount of people getting connected to networks, the security threats that cause massive harm are increasing also.

ICT ITS1	Version:01	Page No.51
	Copyright: Ethiopia Federal TVET Agency	



Network security is a major part of a network that needs to be maintained because information is being passed between computers etc and is very vulnerable to attack. Over the past five years people that manage network security have seen a massive increase of hackers and criminals creating malicious threats that have been pumped into networks across the world.

<b>ICT ITS1</b>	Version:01	Page No.52
	Copyright: Ethiopia Federal TVET Agency	



## Computer and Network threats

### 2.2.1. Viruses and Worms:

- A Virus is a “program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- Viruses can cause a huge amount of damage to computers.
- An example of a virus would be if you opened an email and a malicious piece of code was downloaded onto your computer causing your computer to freeze.
- In relation to a network, if a virus is downloaded then all the computers in the network would be affected because the virus would make copies of itself and spread itself across networks.
- A worm is similar to a virus but a worm can run itself whereas a virus needs a host program to run.

Solution: Install a security suite, such as Kasper sky Total Protection that protects the computer against threats such as viruses and worms.

### 2.2.2. Trojan Horses:

- A Trojan horse is “a program in which malicious or harmful code is contained inside it appears that harmless programming or data in such a way that it can get control and do its chosen form of damage, such as corrupted the file allocation table on your hard disk.
- In a network if a Trojan horse is installed on a computer and tampers with the file allocation table it could cause a massive amount of damage to all computers of that network.
- Solution: Security suites, such as Norton Internet Security, will prevent you from downloading Trojan Horses.

### 2.2.3. SPAM:

- SPAM is “flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.
- SPAM may not be the biggest risk to a network because even though it may get maddening and plentiful it still doesn’t destroy any physical elements of the network.

ICT ITS1	Version:01	Page No.53
	Copyright: Ethiopia Federal TVET Agency	





- Solution: SPAM filters are an effective way to stop SPAM, these filters come with most of the e-mail providers on line. Also you can buy a variety of SPAM filters that work effectively.

#### **2.2.4. Phishing:**

- Phishing is “an e-mail fraud method in which the performer sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients.
- phishing is one of the worst security threats over a network because a lot of people that use computers linked up to a network are unpaid and would be very vulnerable to giving out information that could cause situations such as theft of money or identity theft.
- Solution: Similar to SPAM use Phishing filters to filter out this unwanted mail and to prevent threat.

#### **2.2.5. Packet Sniffers:**

- A packet sniffer is a device or program that allows listen on traffic traveling between networked computers. The packet sniffer will capture data that is addressed to other machines, saving it for later analysis.
- In a network a packet sniffer can filter out personal information and this can lead to areas such as identity theft so this is a major security threat to a network.
- Solution: “When strong encryption is used, all packets are unreadable to any but the destination address, making packet sniffers useless. So one solution is to obtain strong encryption.

#### **2.2.6. Maliciously Coded Websites:**

- Some websites across the net contain code that is malicious.
- Malicious code is “Programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computer system.
- Solution: Using a security suite, such as AVG, can detect infected sites and try to prevent the user from entering the site.

#### **2.2.7. Password Attacks:**

<b>ICT ITS1</b>	Version:01	Page No.54
	Copyright: Ethiopia Federal TVET Agency	



- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas.
- Many systems on a network are password protected and hence it would be easy for a hacker to hack into the systems and steal data.
- This may be the easiest way to obtain private information because you are able to get software online that obtains the password for you.
- Solution: At present there is no software that prevents password attacks.

### **2.2.8. Hardware Loss and Residual Data Fragments:**

- Hardware loss and residual data fragments are a growing worry for companies, governments etc.
- An example this is if a number of laptops get stolen from a bank that have client details on them, this would enable the thief's to get personal information from clients and maybe steal the clients identities.
- This is a growing concern and as of present the only solution is to keep data and hardware under strict surveillance.

### **2.2.9. Shared Computers:**

- Shared computers are always a threat.
- Shared computers involve sharing a computer with one or more people.
- The following are a series of tips to follow when sharing computers: "Do not check the "Remember my ID on this computer" box
- Never leave a computer unattended while signed-in ... Always sign out completely ... Clear the browsers cache ... Keep an eye out for "shoulder surfers" ... Avoid confidential transactions ... Be wary of spy ware ... Never save passwords ... Change your password often.

### **2.2.10. Zombie Computers and Botnets:**

- A zombie computer or "drone" is a computer that has been secretly compromised by hacking tools which allow a third party to control the computer and its resources remotely.
- A hacker could hack into a computer and control the computer and obtain data.

<b>ICT ITS1</b>	Version:01	Page No.55
	Copyright: Ethiopia Federal TVET Agency	



- Solution: Antivirus software can help prevent zombie computers.

**Solution:** Network Intrusion Prevention (NIP) systems can help prevent botnets

### 2.3. Explain web security

Web security is important because so many people visit the World Wide Web every day. Some of the features that make the web useful and entertaining can also make it harmful to a computer.

Tools that are used to make web pages more powerful and versatile are: -

- **ActiveX** – Technology created by Microsoft to control interactivity on web pages. If ActiveX is on a page, an applet or small program has to be downloaded to gain access to the full functionality.
- **Java** – Programming language that allows applets to run within a web browser. Examples of applets include a calculator or a counter.
- **JavaScript** – Programming language developed to interact with HTML source code to allow interactive websites. Examples include a rotating banner or a popup window.

Attackers may use any of these tools to install a program on a computer. To prevent against these attacks, most browsers have settings that force the computer user to authorize the downloading or use of ActiveX, Java, or JavaScript.

### 2.4. Define adware, spyware, and grayware

**Adware** is a software program that displays advertising on your computer. Adware is usually distributed with downloaded software. Most often, adware is displayed in a popup window. Adware popup windows are sometimes difficult to control and will open new windows faster than users can close them.

**Grayware** or malware is a file or program other than a virus that is potentially harmful. Many grayware attacks are phishing attacks that try to persuade the reader to unknowingly provide attackers with access to personal information. As you fill out an online form, the data is sent to the attacker. Grayware can be removed using spyware and adware removal tools.

**Spyware**, a type of grayware, is similar to adware. It is distributed without any user intervention or knowledge. Once installed, the spyware monitors activity on the computer. The spyware then sends this information to the organization responsible for launching the spyware.

### 2.5. Explain Denial of Service

Denial of service (DoS) is a form of attack that prevents users from accessing normal services, such as e-mail and a web server, because the system is busy responding to abnormally large

ICT ITS1	Version:01	Page No.56
	Copyright: Ethiopia Federal TVET Agency	



amounts of requests. DoS works by sending enough requests for a system resource that the requested service is overloaded and ceases to operate.

Common DoS attacks include the following:

- Ping of death – A series of repeated, larger than normal pings that crash the receiving computer
- E-mail bomb – A large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing it

Distributed DoS (DDoS) is another form of attack that uses many infected computers, called zombies, to launch an attack. With DDoS, the intent is to obstruct or overwhelm access to the targeted server. Zombie computers located at different geographical locations make it difficult to trace the origin of the attack.

<b>ICT ITS1</b>	Version:01	Page No.57
	Copyright: Ethiopia Federal TVET Agency	



Self Check 2	Choose Test
--------------	-------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. choose the best answer from the following question**

\_\_\_\_\_ 1. \_\_\_\_\_ the prevention and protection of (computer) assets from unauthorized access,

use, alteration, degradation, destruction, and other threats.

A/Network Security    B/Computer Security    C/Network threat    D/Protocol

\_\_\_\_\_ 2. \_\_\_\_\_ is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

A/Packet Sniffers    B/Phishing    C/SPAM    D/Viruses

\_\_\_\_\_ 3. \_\_\_\_\_ an e-mail fraud method in which the performer sends out legitimate-looking

emails in an attempt to gather personal and financial information from recipients.

A/Packet Sniffers    B/Phishing    C/SPAM    D/Viruses

\_\_\_\_\_ 4. \_\_\_\_\_ is a device or program that allows listen on traffic traveling between networked computers.

A/Viruses    B/Packet Sniffers    C/Phishing    D/SPAM

\_\_\_\_\_ 5. \_\_\_\_\_ is flooding the Internet with many copies of the same message, in an attempt

to force the message on people who would not otherwise choose to receive it.

A/Viruses    B/Packet Sniffers    C/SPAM    D/Phishing

**Note: Satisfactory rating – 2 points**

**Unsatisfactory - below 2 points**

You can ask you teacher for the copy of the correct answers.

<b>ICT ITS1</b>	Version:01	Score = _____	
	Copyright: Ethiopia Federal TVET Agency	Rating: _____	Page No.58



## Answer Sheet

<b>ICT ITS1</b>	Version:01	Page No.59
	Copyright: Ethiopia Federal TVET Agency	



### 3.1. Physical monitoring threats

Use the following Physical threats controlling :-

- Fence
- Guards
- Gate locks
- Lock devices(network device and computers)
- **Authentication (Password):** Password prevention is also very vital. One of the best mechanisms is to ascertain that crasher can't even gain access to the coded password.
- **Organizational policies**

#### **Physical security:** Physical Security

Your organization should be aware how physically secure every aspect of its network is because if an intruder gets physical access, they can get your data. Be sure the organization properly secures locations and consider the following:

- **Servers** - Contain your data and information about how to access that data.
- **Workstations** - Man contain some sensitive data and can be used to attack other computers.
- **Routers, switches, bridges, hubs** and any other network equipment may be used as an access point to your network.
- **Network wiring and media** and where they pass through may be used to access your network or place a wireless access point to your network.
- **External media** which may be used between organizational sites or to other sites the organization does business with.
- Locations of staff that may have information that a hostile party can use.
- Some employees may take data home or may take laptops home or use laptops on the internet from home then bring them to work. Any information on these laptops should be considered to be at risk and these laptops should be secure according to proper policy when connected externally on the network.



### 3.2. Threats to Security

- Internal threats - employees of the organization.
- Deliberate data damage - "just for fun" or with more shady intent, some people might delight in corrupting data or deleting it completely.
- Industrial intelligence - the process of a person retrieving data from a server for a purpose.
- Physical equipment theft - If an important piece of equipment is stolen (for example, the server or a backup tape), the intruder will have access to your data.
- A firewall is a system or group of systems that controls the flow of traffic between two networks. The most common use of a firewall is to protect a private network from a public network such as the Internet.

### 3.3. Protect your password.

Never share your password with anyone, not even a relative or colleague. If another person has your password, they can, for all computer purposes, be you. This extends far beyond simply reading your email.

It's very important to use different passwords for different systems. This limits the damage a malicious person can do should a password fall into the wrong hands.

Following are some measures that you can take in order to minimize the risks associated with malicious human threats:

- **Data Storage in Safe Locations:** Keep your data in safe and secure locations that have limited access to others.
- **Virus and Spyware Protection:** You must open an e-mail attachment or install any software from a Web site with caution. The most reliable way is to install antivirus and anti-spyware software from a reputable vendor.
- **Human Errors:** Many times, damage to a computer is due to unintentional human error. For example, you may accidentally delete an important file, causing the computer to malfunction.
- **Hardware Damage:** Computer components, being delicate, run the risk of getting damaged due to carelessness..
- **Protecting hardware from accidental and environmental damages:** You can take various measures to avoid any unintentional damage to your computer. Keep the computer in an area

ICT ITS1	Version:01	Page No.61
	Copyright: Ethiopia Federal TVET Agency	





that is dust-free, free from vibration, and out of the way of possible impact, should be well-ventilated to prevent any damage due to heat.

- **Backing up Data:** Regularly back up important computer data. Creating multiple copies of data provides protection against loss of data due to accidental erasure or destruction of data.

### **Identify security procedures**

A security plan should be used to determine what will be done in a critical situation. Security plan policies should be constantly updated to reflect the latest threats to a network. A security plan with clear security procedures is the basis for a technician to follow. Security plans should be reviewed on a yearly basis.

There are different security strategies

- ✓ Privacy
- ✓ Authentication
- ✓ Authorization and integrity

**Privacy** is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes.

**Authentication** is the act of confirming the truth of an attribute of a datum or entity.

**Authorization** is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed [access](#) to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth).

**Integrity** is a concept of [consistency](#) of actions, values, methods, measures, principles, expectations, and outcomes. In ethics, integrity is regarded as the [honesty](#) and [truthfulness](#) or [accuracy](#) of one's actions.

<b>ICT ITS1</b>	Version:01	Page No.62
	Copyright: Ethiopia Federal TVET Agency	



<b>ICT ITS1</b>	Version:01	Page No.63
	Copyright: Ethiopia Federal TVET Agency	



Self Check 3

Write Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. Write method Physical threats controlling ?
  
2. Write some measures that you can take in order to minimize the risks associated with malicious human threats?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.64
	Copyright: Ethiopia Federal TVET Agency	



#### 4.1. Data Encryption

Encrypting data uses codes and ciphers. Traffic between resources and computers on the network can be protected from attackers monitoring or recording transactions by implementing encryption. It may not be possible to decipher captured data in time to make any use of it.

**Virtual Private Network (VPN)** uses encryption to protect data. A VPN connection allows a remote user to safely access resources as if their computer is physically attached to the local network.

#### 4.2. Port Protection

Every communication using TCP/IP is associated with a port number. HTTPS, for instance, uses port 443 by default. A firewall is a way of protecting a computer from intrusion through the ports. The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured. Data being transported on a network is called traffic.

#### 4.3. Data Backups

Data backup procedures should be included in a security plan. Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster such as a fire or flood.

Backing up data is one of the most effective ways of protecting against data loss. Here are some considerations for data backups:

- **Frequency of backups** – Backups can take a long time. Sometimes it is easier to make a full backup monthly or weekly, and then do frequent partial backups of any data that has changed since the last full backup. However, spreading the backups over many recordings increases the amount of time needed to restore the data.



- **Storage of backups** – Backups should be transported to an approved offsite storage location for extra security. The current backup media is transported to the offsite location on a daily, weekly, or monthly rotation as required by the local organization.
- **Security of backups** – Backups can be protected with passwords. These passwords would have to be entered before the data on the backup media could be restored.

#### 4.4. Implementing encryption Facilities

One of the most effective ways to eliminate data loss or theft is to encrypt the data as it travels across the network. However, not all data protection solutions are created equal. While most solutions offer standard AES 256-bit encryption, there are other attributes that must be considered:

Some of encryption facilities are: -

- **Public Key Infrastructure (PKI)** is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke [digital certificates](#).<sup>[1]</sup> In [cryptography](#), a PKI is an arrangement that binds [public keys](#) with respective user identities by means of a [certificate authority](#) (CA). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures [non-repudiation](#).
- **Pretty Good Privacy (PGP)** is a popular program used to [encrypt](#) and decrypt e-mail over the Internet. It can also be used to send an encrypted [digital signature](#) that lets the receiver verify the sender's identity and know that the message was not changed en route. Available both as [freeware](#) and in a low-

ICT ITS1	Version:01	Page No.66
	Copyright: Ethiopia Federal TVET Agency	

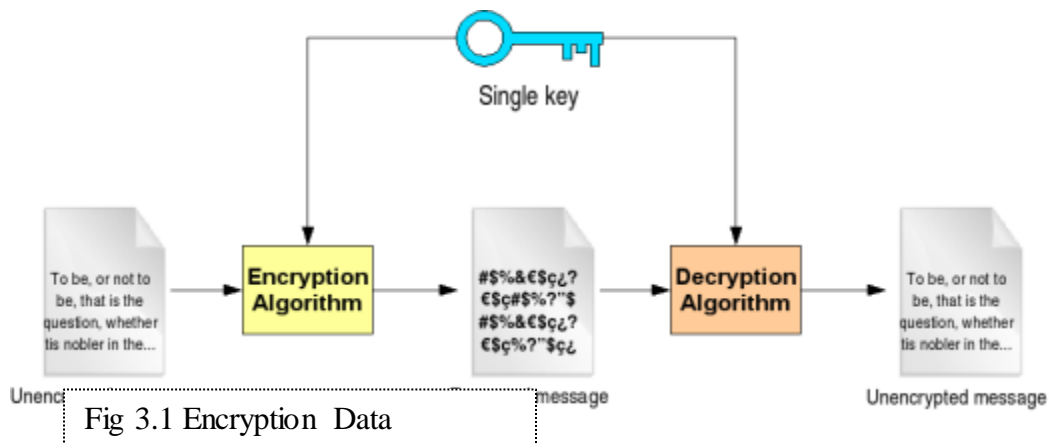


cost commercial version, PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations.

#### 4.5. Symmetric and Asymmetric ciphers

- In a **symmetric cipher**, both parties must use the same key for encryption and decryption. This means that the encryption key must be shared between the two parties before any messages can be decrypted. Symmetric systems are also known as shared secret systems or private key systems. Symmetric ciphers are significantly faster than asymmetric ciphers, but the requirements for key exchange make them difficult to use.
- In an **asymmetric cipher**, the encryption key and the decryption keys are separate. In an asymmetric system, each person has two keys. One key, the public key, is shared publicly. The second key, the private key, should never be shared with anyone.

When you send a message using asymmetric cryptography, you encrypt the message using the recipients' public key. The recipient then decrypts the message using his private key. That is why the system is called asymmetric.



Because asymmetric ciphers tend to be significantly more computationally intensive, they are usually used in combination with symmetric ciphers to implement effect public key cryptography. The asymmetric cipher is used to encrypt a session key and the encrypted session key is then used to encrypt the actual message.

Symmetric ciphers are the oldest and most used cryptographic ciphers. In a symmetric cipher, the key that decipheres the cipher text is the same as (or can be

<b>ICT ITS1</b>	Version:01	Page No.67
	Copyright: Ethiopia Federal TVET Agency	



easily derived from) the key enciphers the clear text. This key is often referred to as the secret key. The most widely used symmetric ciphers are DES and AES.

Unlike a symmetric cipher, an asymmetric cipher uses two keys: one key that is kept secret and known to only one person (the private key) and another key that is public and available to everyone (the public key). The two keys are mathematically interrelated, but it's impossible to derive one key from the other. Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.

What are the advantages and disadvantages of using an asymmetric cipher instead of a symmetric cipher?

- An important advantage of asymmetric ciphers over symmetric ciphers is that no secret channel is necessary for the exchange of the public key. The receiver needs only to be assured of the authenticity of the public key. Symmetric ciphers require a secret channel to send the secret key—generated at one side of the communication channel—to the other side.
- Asymmetric ciphers also create lesser key-management problems than symmetric ciphers. Only  $2n$  keys are needed for  $n$  entities to communicate securely with one another. In a system based on symmetric ciphers, you would need  $n(n - 1)/2$  secret keys. In a 5000-employee organization, for example, the companywide deployment of a symmetric crypto-based security solution would require more than 12 million keys. The deployment of an asymmetric solution would require only 10,000 keys.
- A disadvantage of asymmetric ciphers over symmetric ciphers is that they tend to be about "1000 times slower." By that, I mean that it can take about 1000 times more CPU time to process an asymmetric encryption or decryption than a symmetric encryption or decryption.
- Another disadvantage is that symmetric ciphers can be cracked through a "brute-force" attack, in which all possible keys are attempted until the right key is found.

Because of these characteristics, asymmetric ciphers are typically used for data authentication (through digital signatures), for the distribution of a symmetric bulk

<b>ICT ITS1</b>	Version:01	Page No.68
	Copyright: Ethiopia Federal TVET Agency	



encryption key (aka a digital envelope), for non-repudiation services, and for key agreement. Symmetric ciphers are used for bulk encryption.

- 4.6. Sniffers** monitor network data. A sniffer can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Sniffers usually act as network probes or "snoops." They examine network traffic, making a copy of the data without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels including Ethernet frames.
- 4.7. Secure Shell (SSH)** is a [network protocol](#) for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a [secure channel](#) over an insecure network: a server and a client (running [SSH server](#) and [SSH client](#) programs, respectively).<sup>[1]</sup> The protocol specification distinguishes two major versions that are referred to as SSH-1 and SSH-2.
- 4.8. Deslogin** is a remote login program which may be used safely across insecure networks. With deslogin, you may log into a secure remote host from a secure local host without worry about your login password or session information being made visible across the network. Deslogin is a simple stand-alone client and server, which may be used on machines which don't have more sophisticated security packages such as SPX or Kerberos. No centralized key distribution package is required. Unlike unix Login programs, authentication relies upon arbitrarily long pass phrases rather than eight-character user passwords.
- 4.9. PKZIP** is an archiving tool originally written by [Phil Katz](#) and marketed by his company PKWARE, Inc. The common "PK" prefix used in both PKZIP and [PKWARE](#) stands for "Phil Katz".
- [Secure Sockets Layer \(SSL\)](#) a protocol for encrypting information over the Internet
- 4.10. A digital signature or digital signature scheme** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

ICT ITS1	Version:01	Page No.69
	Copyright: Ethiopia Federal TVET Agency	





Self Check 4

Write Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. Define Data Encryption?
2. Write types Data Backups?
3. Define Secure Shell (SSH)?
4. What the difference between Symmetric and Asymmetric ciphers?

**Note: Satisfactory rating – 2 points**

**Unsatisfactory - below 2 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.70
	Copyright: Ethiopia Federal TVET Agency	



Information Sheet – 5	Preparing and presenting an audit report and recommendation
-----------------------	---

### 5.1. Introduction to Multiple layer of security

There are multiple layers of security in a network, including physical, wireless, and data. Each layer is subject to security attacks. The technician needs to understand how to implement security procedures to protect equipment and data.



Fig 3.2 Multiple Layer

#### Explain what is required in a basic local security policy

Though local security policies may vary between organizations, there are questions all organizations should ask:

- What assets require protection?
- What are the possible threats?
- What to do in the event of a security breach?

A security policy should describe how a company addresses security issues:

ICT ITS1	Version:01	Page No.71
	Copyright: Ethiopia Federal TVET Agency	



- Define a process for handling network security incidents
- Define a process to audit existing network security
- Define a general security framework for implementing network security
- Define behaviors that are allowed
- Define behaviors that are prohibited
- Describe what to log and how to store the logs: Event Viewer, system log files, or security log files
- Define network access to resources through account permissions
- Define authentication technologies to access data: usernames, passwords, biometrics, smart cards

### **Explain the tasks required to protect physical equipment**

Physical security is as important as data security. When a computer is taken, the data is also stolen.

There are several methods of physically protecting computer equipment,

- Control access to facilities
- Use cable locks with equipment
- Keep telecommunication rooms locked
- Fit equipment with security screws
- Use security cages around equipment
- Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment

For access to facilities, there are several means of protection:

- Card keys that store user data, including level of access
- Berg connectors for connecting to a floppy drive
- Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
- Posted security guard

<b>ICT ITS1</b>	Version:01	Page No.72
	Copyright: Ethiopia Federal TVET Agency	



- Sensors, such as RFID tags, to monitor equipment



Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.*

**I. Write the answer briefly**

1. Define security policy should describe a company addresses security issues?

2. Write methods of physically protecting computer equipment?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask your teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_



### 6.1. Describe ways to protect data

The value of physical equipment is often far less than the value of the data it contains. The loss of sensitive data to a company's competitors or to criminals may be costly. Such losses may result in a lack of confidence in the company and the dismissal of computer technicians in charge of computer security. To protect data, there are several methods of security protection that can be implemented.

### 6.2. Password Protection

Password protection can prevent unauthorized access to content. Attackers are able to gain access to unprotected computer data. All computers should be password protected. Two levels of password protection are recommended:

- BIOS – Prevents BIOS settings from being changed without the appropriate password
- Login – Prevents unauthorized access to the network

Network logins provide a means of logging activity on the network and either preventing or allowing access to resources. This makes it possible to determine what resources are being accessed. Usually, the system administrator defines a naming convention for the usernames when creating network logins. A common example of a username is the first initial of the person's first name and then the entire last name. You should keep the username naming convention simple so that people do not have a hard time remembering it.

When assigning passwords, the level of password control should match the level of protection required. A good security policy should be strictly enforced and include, but not be limited to, the following rules:

- Passwords should expire after a specific period of time.

<b>ICT ITS1</b>	Version:01	Page No.75
	Copyright: Ethiopia Federal TVET Agency	



- Passwords should contain a mixture of letters and numbers so that they cannot easily be broken.
- Password standards should prevent users from writing down passwords and leaving them unprotected from public view.
- Rules about password expiration and lockout should be defined. Lockout rules apply when an unsuccessful attempt has been made to access the system or when a specific change has been detected in the system configuration.

To simplify the process of administrating security, it is common to assign users to groups, and then to assign groups to resources. This allows the access capability of users on a network to be changed easily by assigning or removing the user from various groups. This is useful when setting up temporary accounts for visiting workers or consultants, giving you the ability to limit access to resources.

### 6.3. Explain social engineering

A *social engineer* is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information. Often, the social engineer gains the confidence of an employee and convinces the employee to divulge username and password information.

Here are some basic precautions to help protect against social engineering:

- Never give out your password
- Always ask for the ID of unknown persons
- Restrict access of unexpected visitors
- Escort all visitors
- Never post your password in your work area
- Lock your computer when you leave your desk
- Do not let anyone follow you through a door that requires an access card

### 6.4. Explain TCP/IP attacks

ICT ITS1	Version:01	Page No.76
	Copyright: Ethiopia Federal TVET Agency	



TCP/IP is the protocol suite that is used to control all of the communications on the Internet. Unfortunately, TCP/IP can also make a network vulnerable to attackers.

<b>ICT ITS1</b>	Version:01	Page No.77
	Copyright: Ethiopia Federal TVET Agency	





Self Check 6

Write Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. List two levels of password protection are recommended?
2. Write some basic precautions to help protect against social engineering?

**Note: Satisfactory rating – 1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

**Instruction Sheet****LG30: Establish maintenance practices**

This learning guide is developed to provide you the necessary information regarding the

Following content coverage and topics –

- Determining maintenance requirements specified by the equipment manufacturer.
- Producing maintenance schedules
- Performing diagnostic function
- Configuring software security settings
- Determining unserviceable components
- Using the operating system and third-party diagnostic tools

This guide will also assist you to attain the learning outcome stated in the cover page.

Specifically, upon completion of this Learning Guide, you will be able to –

- Maintenance requirements specified by the equipment manufacturer are determined.
- Maintenance schedules including removal of dust and grease build -up are produced
- Diagnostic functions including replacing suspect components with other serviceable components and reloading of associated software are performed
- Software security settings to prevent destructive software from infecting the computer are configured
- Unserviceable components are determined whether replaceable through warranty, replacement or upgrade
- Diagnostic functions are performed using the operating system and third-party diagnostic tools

**Learning Instructions:**

10. Read the specific objectives of this Learning Guide.
11. Follow the instructions described below 3 to 6.
12. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3
13. , Sheet 4 , Sheet 5 and Sheet 6” in **page 1,4,12, 18, 22 and 57** respectively.

<b>ICT ITS1</b>	Version:01	Page No.79
	Copyright: Ethiopia Federal TVET Agency	



14. Accomplish the “Self-check 1, Self-check 2, Self-check 3 Self-check 4, Self-check 5 and Self-check 6” , in page , 3,11,17,21,56,and 64 respectively

Information Sheet – 1	Determining maintenance requirements specified by the equipment manufacturer.
-----------------------	---

### 1.1 Maintenance requirement

Maintenance requirement is the materials or tools that are important to maintain specific equipment.

Maintenance requirement may include but not limited to: -

- Caution
- Attention

**Attention** is more than just noticing incoming stimuli. It involves a number of processes including filtering out perceptions, balancing multiple perceptions and attaching emotional significance to these perceptions.

There are two major forms of attention: *passive* and *active*. *Passive* attention refers to the involuntary process directed by external events that stand out from their environment, such as a bright flash, a strong odor, or a sudden loud noise. We might say that because passive attention is involuntary, it is easy. *Active* attention is voluntary and is guided by alertness, concentration, interest and needs such as curiosity and hunger.

**Personal computers** (PCs), also called microcomputers, are the most popular type of computer in use today. The PC is a small-sized, relatively inexpensive computer designed for an individual user. Today, the world of PCs is basically divided between IBM-compatible and Macintosh-compatible machines, named after the two computer manufacturers. Computers may be called ‘desktop’ computers, which stay on the desk, or ‘laptop’ computers, which are lightweight and portable. Organisations and individuals use PCs for a wide range of tasks, including word processing, accounting, desktop publishing, preparation and delivery of presentations, organisation of spreadsheets and database

<b>ICT ITS1</b>	Version:01	Page No.80
	Copyright: Ethiopia Federal TVET Agency	



management. Entry-level PCs are much more powerful than a few years ago, and today there is little distinction between PCs and workstations.

## Switches

- On the surface, a [switch](#) looks much like a hub. Despite their similar appearance, switches are far more efficient than hubs and are far more desirable for today's network environments.
- As with a hub, computers connect to a switch via a length of twisted-pair cable. Multiple switches are often interconnected to create larger networks.



Fig:-4.1. Switch

- Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected.
- It looks at the *Media Access Control (MAC)* addresses of the devices connected to it to determine the correct port. A MAC address is a unique number that is stamped into every NIC. By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically.

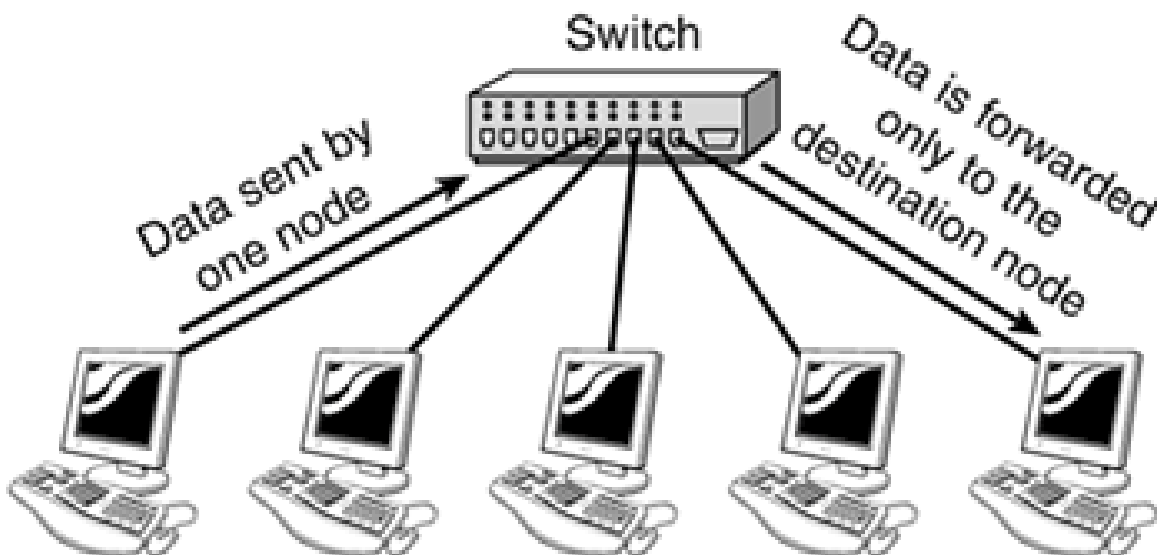




Fig:-4.2. Media Access Control(MAC)



Self Check 1

Write Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

3. Define Maintenance requirement ?

4. Define Personal computer?

5. Define Switch?

**Note: Satisfactory rating – 2 points**

**Unsatisfactory - below 2 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_



## Information Sheet – 2

## Producing maintenance schedules

### 2.1. Maintenance Schedule

Maintenance Schedule is a plan or procedures that are used to maintain equipment and it must be programmed with time of intervals. Maintenance schedules including removal of dust, grease build-up and etc.

Maintenance scheduling can be planned or prepared as:-

- Onsite response
- Remote diagnostic

**Onsite response** is one of maintenance schedule that display the plan or procedures from the internet.

**Remote diagnostics** refers to the ability to evaluate the current status of electronic equipment from a remote location. The process involves the establishment of some type of wired or wireless communication between the two points in order for the remote analysis to take place.

**Remote diagnostics** is the act of [diagnosing](#) a given symptom, issue or problem from a distance

### 2.2. MAINTENANCE PLANNING AND SCHEDULING

Effective planning and scheduling contribute significantly to the following:

- Reduced maintenance cost.
- Improved utilization of the maintenance workforce by reducing delays and interruptions.

ICT ITS1	Version:01	Page No.84
	Copyright: Ethiopia Federal TVET Agency	



- Improved quality of maintenance work by adopting the best methods and procedures and assigning the most qualified workers for the job.

### 2.2.1. Planning and Scheduling Objectives

- Minimizing the idle time of maintenance workers.
- Maximizing the efficient use of work time, material, and equipment.
- Maintaining the operating equipment at a responsive level to the need of production in terms of delivery schedule and quality.

### 2.2.2. Classification of Maintenance Work According to Planning and Scheduling Purposes

- **Routine maintenance:** are maintenance operations of a periodic nature. They are planned and scheduled and in advance. They are covered by blanket orders.
- **Emergency or breakdown maintenance:** interrupt maintenance schedules in order to be performed. They are planned and scheduled as they happened.
- **Design modifications:** are planned and scheduled and they depend on eliminating the cause of repeated breakdowns.
- **Scheduled overhaul and shutdowns of the plant:** planned and scheduled in advanced.
- **Overhaul, general repairs, and replacement:** planned and scheduled in advanced.
- **Preventive maintenance:** planned and scheduled in advanced.
- An essential part of planning and scheduling is to forecast future work and to balance the workload between these categories.
- The maintenance management system should aim to have over 90% of the maintenance work planned and scheduled.

### 2.2.3. Planning

Planning is the process by which the elements required to perform a task are determined in advance of the job start.

ICT ITS1	Version:01	Page No.85
	Copyright: Ethiopia Federal TVET Agency	





- It comprises all the functions related to the preparation of:
  - The work order
  - Bill of material
  - Purchase requisition
  - Necessary drawings
  - Labor planning sheet including standard times
  - All data needed prior to scheduling and releasing the work order.
- Good planning is a prerequisite for sound scheduling.

### **2.2.3.1. Planning Procedures**

- Determine the job content.
- Develop work plan. This entails the sequence of the activities in the job and establishing the best methods and procedures to accomplish the job.
- Establish crew size for the job.
- Plan and order parts and material.
- Check if special tools and equipment are needed and obtain them.
- Assign workers with appropriate skills.
- Review safety procedures.
- Set priorities for all maintenance work.
- Assign cost accounts.
- Complete the work order.
- Review the backlog and develop plans for controlling it.
- Predict the maintenance load using effective forecasting technique.

### **2.2.3.2. Basic Levels of Planning Process (Depend on The Planning Horizon)**

- Long-rang planning: it covers a period of 3 to 5 years and sets plans for future activities and long-range improvement.
- Medium-range planning: it covers a period of 1 month to 1 year.
- Short-rang planning: it covers a period of 1 day to 1 week. It focuses on the determination of all the elements required to perform maintenance tasks in advance.
- **Long and Medium-Range Planning**

<b>ICT ITS1</b>	Version:01	Page No.86
	Copyright: Ethiopia Federal TVET Agency	



Needs to utilize the following:

- Sound forecasting techniques to estimate the maintenance load.
- Reliable job standards times to estimate staffing requirements.
- Aggregate planning tools such as linear programming to determine resource requirements.
- **Long-Range Planning**
  - sets plans for future activities and long-range improvement.
- **Medium-Range Planning**
  - Specify how the maintenance workers will operate.
  - Provide details of major overhauls, construction jobs, preventive maintenance plans, and plant shutdowns.
  - Balances the need for staffing over the period covered.
  - Estimates required spare parts and material acquisition.
- **Short-Range Planning**

It focuses on the determination of all the elements required to perform maintenance tasks in advance.

#### 2.2.4. Scheduling

- Is the process by which jobs are matched with resources and sequenced to be executed at a certain points in time.
- Scheduling deals with the specific time and phasing of planned jobs together with the orders to perform the work, monitoring the work, controlling it, and reporting on job progress.
- Successful planning needs a feedback from scheduling.

#### **Reliable Schedule Must Take Into Consideration**

- A job priority ranking reflecting the criticality of the job.
- The availability of all materials needed for the work order in the plant.
- The production master schedule.
- Realistic estimates and what is likely to happen.
- Flexibility in the schedule.

#### **Elements of Sound Scheduling**

ICT ITS1	Version:01	Page No.87
	Copyright: Ethiopia Federal TVET Agency	



Requirements for effective scheduling:

- Written work orders that are derived from a well-conceived planning process. (Work to be done, methods to be followed, crafts needed, spare parts needed, and priority).
- Time standards.
- Information about craft availability for each shift.
- Stocks of spare parts and information on restocking.
- Information on the availability of special equipment and tools necessary for maintenance work.
- Access to the plant production schedule and knowledge about when the facilities will be available for service without interrupting production schedule.
- Well-define priorities for maintenance work.
- Information about jobs already scheduled that are behind the schedule (backlog).

### **Maintenance Schedule Can be Prepared at Three Levels (Depend on The Time Horizon)**

- Long-range (master) schedule
- Weekly schedule
- Daily schedule

### **Long-Range (master) Schedule**

- Covering a period of 3 months to 1 year.
- Based on existing maintenance work orders (blanket work order, backlog, PM, anticipated EM).
- Balancing long-term demand for maintenance work with available resources.
- Spare parts and material could be identified and ordered in advance.
- Subject to revision and updating to reflect changes in the plans and maintenance work.

### **Weekly Schedule**

- Covering 1 week.

<b>ICT ITS1</b>	Version:01	Page No.88
	Copyright: Ethiopia Federal TVET Agency	



- Generated from the master schedule.
- Takes into account current operations schedules and economic considerations.
- Allow 10% to 15% of the workforce to be available for emergency work.
- The schedule prepared for the current week and the following one in order to consider the available backlog.
- The work orders scheduled in this week are sequenced based in priority.
- CPM and integer programming techniques can be used to generate a schedule.

### **Daily Schedule**

- Covering 1 day.
- Generated from weekly schedule.
- Prepared the day before.
- Interrupted to perform EM.
- Priorities are used to schedule the jobs.

### **Scheduling Procedures (Steps)**

- Sort backlog work orders by crafts.
- Arrange orders by priority.
- Compile a list of completed and carry over jobs.
- Consider job duration, location, travel distance, and the possibility of combining jobs in the same area.
- Schedule multi-craft jobs to start at the beginning of every shift.
- Issue a daily schedule (not for shutdown maintenance).
- Authorize a supervisor to make work assignments (dispatching).

### **Maintenance Job Priority System**

- Priorities are established to ensure that the most critical work is scheduled first.
- It is developed under coordination with operations staff.

<b>ICT ITS1</b>	Version:01	Page No.89
	Copyright: Ethiopia Federal TVET Agency	



- It should be dynamic.
- It must be updated periodically to reflect changes in operation and maintenance strategies.
- It typically includes three to ten levels of priority.

### Priorities of Maintenance Work

Code	Name	Time frame work should start	Type of work
1	Emergency	Work should start immediately	Work that has an immediate effect on safety, environment, quality, or will shut down the operation
2	Urgent	Work should start within 24 h	Work that is likely to have an impact on safety, environment, quality, or shut down the operation
3	Normal	Work should start within 48 h	Work that is likely to impact the production within a week.
4	Scheduled	As scheduled	Preventive maintenance and routine. All programmed work
5	Postponable	Work should start when resources are available or at shutdown period	Work that does not have an immediate impact on safety, health, environment, or the production operations

Table 4.1. Priorities of Maintenance Work

### Scheduling Techniques

The objective of the scheduling techniques is to construct a time chart showing:

- The start and finish for each job.
- The interdependencies among jobs.
- The critical jobs that require special attention and effective monitoring.

Such techniques are:

- Modified Gantt chart
- CPM
- PERT
- Integer and stochastic programming.

### Example

<b>ICT ITS1</b>	Version:01	Page No.90
	Copyright: Ethiopia Federal TVET Agency	



↓Activity	Days of the month (January)															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
A	█															
B					█											
C	█															
D				█												
E				█												
F										█						
G										█						

4.1:- Gantt Chart

Self Check 2	Write Test
--------------	------------

Name: \_\_\_\_\_

Date: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.91
	Copyright: Ethiopia Federal TVET Agency	



*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. If statement is correct say True if statement is incorrect Say False**

1. Maintenance Schedule is a plan or procedures that are used to maintain equipment and it must be programmed with time of intervals.
2. Planning is the process by which the elements required to perform a task are determined in advance of the job start.
3. Medium-rang planning: it covers a period of 3 to 5 years and sets plans for future activities and long-range improvement.

**Note: Satisfactory rating –2 points**

**Unsatisfactory - below 2 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.92
	Copyright: Ethiopia Federal TVET Agency	



### 3.1. Diagnostic functions

It includes but not limited

- Replacing suspected components
- Upgrade components
- Reloading software's

#### 3.1. Replacing suspected components

Computer hardware or components that can be replaced are: -

- Motherboards
- CMOS battery
- Central processing Unit (CPU)
- Drives (floppy, hard disk, CD-ROM)
- Interface cards
- Fax, modem cards
- RAM

#### 3.2. Upgrade components

Computer hardware or components that can be upgrade are: -

- Central processing Unit (CPU)
- RAM

### How to Replace a Motherboard

Replacing a motherboard takes a moderate understanding of how the components in your computer are assembled. Before replacing the motherboard, back up all your information to ensure it won't get lost, and go to your motherboard's manufacturer to download any updated drivers that may need to be installed after you install the new motherboard. This will help ensure that changing your motherboard is a success.

### Instructions

<b>ICT ITS1</b>	Version:01	Page No.93
	Copyright: Ethiopia Federal TVET Agency	





1. Unplug all power sources to your computer, and remove the casing from your computer. Set aside all screws and small pieces in a bowl so nothing will get lost.
2. Remove all the connectors to the motherboard. This may be your video card, data cables from the hard drives and adapters. Label each one before removing so you can remember exactly where they will attach on your new motherboard.
3. Take out the old motherboard carefully by removing the screws and sliding it out. There is generally little clearance on the sides of the motherboard, so use caution when removing it so nothing gets broken.
4. Compare the new and old motherboards to ensure they're the same. If the new motherboard has cut-outs for integrated sound or game ports, punch out the holes so the wires can fit through them. Do this carefully with a Phillips-head screwdriver or pliers.
5. Place the new motherboard in the case. Double-check to make sure it lines up properly in the computer case before connecting it. Use the seven screws that are included to install the motherboard.
6. Attach the adapters, drives and power connectors to the new motherboard. Locate where you labeled everything before, and install them in the exact same places.
7. Put the computer case back on and turn the power supply back on. If the computer doesn't start up properly, remove the case and double-check to ensure that all the adapters, drives and power supply cords are in the correct position and are tightened securely.

#### Tips & Warnings

- Avoid creating static electricity charges while you're installing the new motherboard by wearing a static-free wristband or grounding yourself often by touching the metal case.

#### How to Replace a CPU

A computer's central processing unit, or CPU, can be thought of as the computer's brain, which carries out the majority of the calculations and processes needed to make the computer run. As computers age, processors may run more slowly due to power surges, overheating and other stress-induced damage. Replacing a used CPU with a new one can often increase performance, but it is usually more common to install a CPU upgrade rather than a straight replacement.

<b>ICT ITS1</b>	Version:01	Page No.94
	Copyright: Ethiopia Federal TVET Agency	



## Instructions

### *Things you'll need*

- 
- Screwdriver(s)
  - Replacement CPU
  - Thermal grease or other thermal interface material
1. Turn off the computer and unplug all plugs.
  2. Open the computer's case and set it on its side.
  3. Take off the CPU fan and heat sink. The CPU fan and heat sink will be easy to locate: look for a large fan on top of a fin-like network of metal attached to the motherboard. Depending on your heat sink, you may either have to unscrew it, or undo some plastic clipping mechanisms holding it in place. Sometimes removing the fan first can make removing the heat sink easier. You will likely have to unplug the fan from the motherboard.
  4. Undo the securing lever on the processor mount to release the old CPU. The CPU will be held in by a mounting system that is closed when a small lever is pressed down. Left the lever up and release the CPU.
  5. Remove the old CPU.

<b>ICT ITS1</b>	Version:01	Page No.95
	Copyright: Ethiopia Federal TVET Agency	



6. Put the new CPU in place, hold it down with a finger, and close the lever to lock it in. Do not exert much force on the CPU; you don't have to press hard, but you may have to wiggle it around a little bit to get it to line up properly before closing the lever.
7. Apply thermal grease liberally to the CPU. The CPU needs a thermal interface material between it and the heat sink to transfer heat effectively.
8. Reinstall the heat sink and fan, making sure the thermal grease is touching both the CPU and the heat sink. Plug the fan back into the motherboard.
9. Close the computer case.

### Tips & Warnings

- If you are planning on installing replacement CPU that is different than the original CPU, make sure your motherboard can use it first.
- The interior of a computer is susceptible to electric shock. Guard against carrying a dangerous charge. Touch the metal case of the computer at least every couple of minutes to make sure you don't shock the computer's components

---

### How to Upgrade a Processor

Upgrading the processor in a computer can be one of the easiest ways to give new life to an older, slower machine. While the upgrade itself will take little time or effort, there is significant work that must be done beforehand to ensure that the upgrade is completed successfully.

### Instructions

1. Research the computer that is to receive the new processor. There are many different processors on the market, and they are not all compatible with a particular machine. Visit the website of the computer manufacturer. If the computer was assembled from after-market components, check the website of the company that manufactured the motherboard, or main circuit board, of the computer. Find out the processor brand, the processor family, the processor

<b>ICT ITS1</b>	Version:01	Page No.96
	Copyright: Ethiopia Federal TVET Agency	



and bus speeds that the machine supports, the type of processor socket on the board and the processor cores or revisions that are compatible with the machine.

2. Shop for a compatible processor from either a local retailer or an online store. The processor must meet all the requirements that your research uncovered, otherwise it will likely be incompatible with the machine. As soon as the processor is received, check it against your original order.
3. Install the processor. Disconnect the computer cables and unplug the machine. Move it to a good work area. Open the side of the machine to obtain access to the interior. Before going any further, discharge any static electricity from your body by using a grounding wrist strap or by touching the bare metal of the computer case.
4. Find the processor. It will be one of the largest objects on the motherboard, near the center, and it will be covered by a large heat sink and fan. On each side of the heat sink, there should be a clip or some other fastener securing it to the processor socket. Gently unhook the clips, taking extreme care not to damage the processor socket, and then disconnect the power lead that runs from the fan to the motherboard. The heat sink then can be pulled away from the processor. It may take some force to separate the heat sink from the processor, depending on the type of thermal transfer compound used.
5. Examine the processor. On one side of the processor socket, there will be a metal or plastic arm that is used to secure the processor in the socket. Slide the end of this arm out from the retaining clip, and lift the arm until it is perpendicular to the motherboard. The old processor can then be gently pulled out.
6. Look at the processor socket. There should be one corner that has a small, 45-degree notch, or another distinguishing mark, cut into it. The processor should have a similar mark. Rotate the processor until the mark is in the same corner as the mark on the socket. Once the processor is orientated correctly, line up the pins and slide the processor into the socket. This should require no force at all. If force is used, the processor pins may be bent and the processor permanently damaged. With the processor seated in the socket, the retaining arm may be lowered and clipped into position.
7. Install the heat sink and fan assembly with a thin layer of thermal compound or a thermal pad between it and the processor. This step transfers heat away from the processor to the heat sink,

<b>ICT ITS1</b>	Version:01	Page No.97
	Copyright: Ethiopia Federal TVET Agency	



preventing the processor from overheating. With the heat sink in place, plug the power lead from the fan back into the motherboard.

8. Close the computer. Reconnect the components and test the new upgrade. When everything is done, the computer should be noticeably faster, and it will be able to handle more robust applications and games than it could previously.

<b>ICT ITS1</b>	Version:01	Page No.98
	Copyright: Ethiopia Federal TVET Agency	



Self Check 3

Write Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. Write instruction Replace a Motherboard?

2. Write instruction Replace a CPU?

**Note: Satisfactory rating –1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.99
	Copyright: Ethiopia Federal TVET Agency	



## Information Sheet – 4

## Configuring software security settings

### 4.1. Firewall

In computing, a firewall is software or [firmware](#) that enforces a set of rules about what [data packets](#) will be allowed to enter or leave a network. Firewalls are incorporated into a wide variety of networked devices to filter traffic and lower the risk that malicious packets traveling over the public internet can impact the security of a private network. Firewalls may also be purchased as stand-alone software applications.

The term *firewall* is a metaphor that compares a type of physical barrier that's put in place to limit the damage a fire can cause, with a virtual barrier that's put in place to limit damage from an external or internal cyberattack. When located at the perimeter of a network, firewalls provide low-level network protection, as well as important logging and auditing functions.

While the two main types of firewalls are host-based and network-based, there are many different types that can be found in different places and controlling different activities. A host-based firewall is installed on individual servers and monitors incoming and outgoing signals. A network-based firewall can be built into the cloud's infrastructure, or it can be a virtual firewall service.

### Types of firewalls

Other types of firewalls include [packet-filtering](#) firewalls, [stateful inspection](#) firewalls, [proxy firewalls](#) and next-generation firewalls ([NGFW](#)).

- A packet-filtering firewall examines packets in isolation and does not know the packet's context.
- A stateful inspection firewall examines network traffic to determine whether one packet is related to another packet.
- A proxy firewall inspects packets at the application layer of the Open Systems Interconnection ([OSI](#)) reference model.

ICT ITS1	Version:01	Page No.100
	Copyright: Ethiopia Federal TVET Agency	



An NGFW uses a multilayered approach to integrate enterprise firewall capabilities with an intrusion prevention system ([IPS](#)) and application control.

When organizations began moving from [mainframe](#) computers and dumb clients to the [client-server model](#), the ability to control access to the server became a priority. Before the first firewalls emerged based on work done in the late 1980s, the only real form of network security was enforced through access control lists ([ACL](#)) residing on routers. ACLs specified which Internet Protocol ([IP](#)) addresses were granted or denied access to the network.

The exponential growth of the internet and the resulting increase in connectivity of networks, however, meant that filtering network traffic by IP address alone was no longer enough. Static packet-filtering firewalls, which examine packet headers and use rules to make decisions about what traffic to let through, arguably became the most important part of every network security initiative by the end of the last century.

## How packet-filtering firewalls work

When a packet passes through a packet-filtering firewall, its source and destination address, [protocol](#) and destination [port number](#) are checked. The packet is dropped -- it's not forwarded to its destination -- if it does not comply with the firewall's rule set. For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for Transmission Control Protocol ([TCP](#)) port number 23, the port where a [Telnet](#)server application would be listening.

There are mechanisms that are used to configure security. Some of them are: -

- Install firewall
- Install antivirus
- Install anti-malware
- Install anti-spyware

### 4.1. How to Install Windows XP Firewall

ICT ITS1	Version:01	Page No.101
	Copyright: Ethiopia Federal TVET Agency	





## Instruction

- To get started first click start and open the control panels network connection icon. Click network and Internet Connections. Click the windows firewall icon which should be clearly visible.
- This brings up the windows firewall dialog box. Click the "On" button. This button will stop all intruders from gaining access to your computer. Now click the exceptions tab on top. Put a check mark next to anything there that you wish to use. For example checking file and print share will allow other computers to gain access to your computer and share files and the printer.
- Once you've checked off what you wish to allow click OK and the firewall is set!
- Windows firewall inadequate? Some computer users like a second line of defense while on the Internet. Click on over to Cnets downloads.com to check out their top free personal computer firewalls. Popular firewalls include Zone Alarm and PC Tools Firewalls. Both are free to download.

<b>ICT ITS1</b>	Version:01	Page No.102
	Copyright: Ethiopia Federal TVET Agency	



Self Check 4

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. Define Firewall?
  
  
  
  
  
  
  
  
  
  
2. Write mechanisms that are used to configure security?

**Note: Satisfactory rating –1 points                      Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.103
	Copyright: Ethiopia Federal TVET Agency	



## Information Sheet – 5

## Determining unserviceable components

### 5.1. Troubleshooting Power Sources and Power Protection Devices

This section lists some typical problems related to the system power. This includes external power problems, [power protection devices](#) (surge suppressors, UPSes, etc.) and also the internal power supply.

A couple of general caveats that you should consider whenever you believe you are looking at a power-related problem:

- I strongly recommend the use of a power protection device, especially if you live in an area with bad power or a lot of electrical storms.
- If this is a new system, read [this section describing common problems in newly assembled PCs](#).
- Read these [care instructions related to power](#).

Please choose the problem description best describing the problem you are having.

#### The power supply appears to not be functioning

- **Explanation:** The PC's internal power supply appears not to work at all. The system will not turn on and the power supply itself appears to be dead.
- **Diagnosis:** There is a possibility that the internal power supply has failed; this does happen, especially on older or cheaper PCs. The power supply can be damaged due to electrical storms, overheating or other causes.

#### Recommendation:

- If you have not done so already, you should first verify that it really is the internal power supply causing the PC not to have power, as opposed to an external electrical cause. [Follow this part of the boot process troubleshooting walkthrough](#) to verify the cause of the lack of power.

ICT ITS1	Version:01	Page No.104
	Copyright: Ethiopia Federal TVET Agency	



- If you have an [ATX system](#), double-check the connections from the case power switch to the motherboard. On an ATX system the power switch does not physically turn on the power supply, it just sends a signal to the motherboard to turn on the PC.
- Check *very* carefully for something inside the PC that may have accidentally short-circuited the power supply. One way this can happen is by incorrectly attaching a power connector to a storage drive. Another possibility is incorrect motherboard installation, or something else loose inside the case. If the power supply has been short-circuited, it will detect this immediately and "play dead"; when you resolve the short, the supply should come back up.
- Replace the power supply. On most machines this is not that difficult of a task, and the power supplies themselves are reasonably standardized. However, make sure you get the right [form factor](#) when ordering a replacement.
- [Take the PC in for repair](#).

**I've noticed that the lights flicker occasionally in my office and sometimes when they do, the PC will hang or reboot**

- **Explanation:** The PC is exhibiting instability or strange behavior at the same time that other symptoms of power fluctuation are apparent.
- **Diagnosis:** Low quality input power to the PC is causing it to behave erratically. Flickering lights means either power grid problems (brownouts, electrical storms), poor wiring in the building, or draw from large electricity-using devices, especially air conditioners.

**Recommendation:**

- If you are not using any sort of power protection device, get one and see if it fixes the problem. Even a \$20 surge protector is better than nothing since it will provide some line filtering. If possible, try using a [UPS](#) and see if that solves the problem--it probably will.
- Try the PC in a different location and see if the problem resolves. This will clearly implicate the power coming from the wall.
- If you are in a home with central air conditioning, see if you can tie the light flickering to when the unit comes on. If so, you may want to see if the PC works better on a different circuit. You

ICT ITS1	Version:01	Page No.105
	Copyright: Ethiopia Federal TVET Agency	



may want to consult a qualified electrician if the air conditioner is causing this much draw, or simply get a UPS.

- [Look here for more ideas on system instability.](#)

### **I need to run my PC on a different voltage, but there is no switch to change the line voltage**

- **Explanation:** The PC is currently set to 110 volt input, but needs to be able to run at 220 volts (or vice-versa) and there is no voltage switch on the back of the power supply.
- **Diagnosis:** Sometimes there actually *is* a voltage switch, but it is hidden, either intentionally or unintentionally, under labels or covers on the back of the PC. Otherwise, you will need to use a voltage converter.

### **Recommendation:**

- Check carefully on the back of the power supply for a switch, looking under any labels there (on a new PC, do not remove any labels that warn you about voiding your warranty).
- Use a voltage conversion device. These are sold in electronics shops; Radio Shack is a good place to start. Make sure you ask for something that will work with a PC.
- Replace the power supply with a unit that has selectable voltage. This is a bit of a pain but will certainly solve the problem.

### **There's a squealing or whining sound coming from the power supply when I turn it on**

- **Explanation:** The PC is making a squealing or whining sound, coming from the back of the power supply unit. The sound may be louder when the PC is first started up, and then diminish, or it may get worse as the PC is left on for a period of time.
- **Diagnosis:** Usually, the cause of this problem is the fan on the back of the power supply. It will tend to accumulate dirt over time, and cheaper ones will fail readily. If the fan is making noise now, it will probably fail soon. This usually takes years, but with cheaper power supplies that can be a surprisingly small number of years. Rarely, the problem can be with the internals of the power supply itself.

<b>ICT ITS1</b>	Version:01	Page No.106
	Copyright: Ethiopia Federal TVET Agency	



### Recommendation:

- Look and listen closely at the back of the PC to see if the fan is what is causing the problem. If it appears that the fan is making the noise, [troubleshoot it here](#).
- If you hear a high-pitched whistling sound, this could be coming from components within the power supply. This will require you to either replace the power supply or [take the system in for service](#).

### My UPS is supposed to provide {N} minutes of backup power, but mine cuts out after much less time than that

- **Explanation:** You purchased a [UPS](#) that claimed that it would provide a certain amount of time running on the batteries when the power went down, but the batteries last much less time than what the advertisements claim.
- **Diagnosis:** The advertisements often exaggerate. Unfortunately, just like everything in the industry, claims that have numbers in them tend to be based on best-case ideal world conditions that don't always hold up in the real world. In addition, claims of battery life are based on a particular configuration. Every PC is different and has a different power demand.

### Recommendation:

- Take all numeric advertising claims with a grain of salt.
- Follow the manufacturer's instructions for maximizing battery life. This may include routine maintenance for the device.
- Consult the manufacturer's technical support line for feedback on whether the battery life you are experiencing is normal. It is possible that your device may be defective. If battery life was at one point higher and now has decreased, this could be a defect as well.
- Consider removing devices from your PC that you don't need

### My UPS doesn't provide proper backup power when the line power goes out

- **Explanation:** A UPS is being used on the PC, but when the power goes out the UPS doesn't keep the PC running.

ICT ITS1	Version:01	Page No.107
	Copyright: Ethiopia Federal TVET Agency	



- **Diagnosis:** There is either something wrong internally with the device, or it has been connected or configured incorrectly.

### Recommendation:

- If the unit is making any noises or has LEDs flashing in strange configurations, consult the manufacturer's [technical support](#).
- The unit may be overloaded. If a 400 kVA unit will support your system for 5 minutes on battery backup, this does not mean that a 200 kVA unit will necessarily support it for 2.5 minutes. Once a unit gets too much load on it, it may not work *at all* when the power goes out. You will need a more powerful unit in this case.
- Check the unit physically to make sure that everything is connected properly, there are no tripped circuit breakers, etc.
- Try plugging the PC into a different socket in the device and see if that solves the problem. If it does, the device has a failure with that particular socket and it needs to be repaired or replaced.
- The batteries could be damaged, defective, or discharged. Follow the manufacturer's instructions for ensuring that the batteries are fully charged and see if the problem works properly.
- Consult with the manufacturer of the device for [technical support](#).

ICT ITS1	Version:01	Page No.108
	Copyright: Ethiopia Federal TVET Agency	



## Windows automatically turns off the PC when I tell it to shut down, and I don't want it to (or vice-versa)

- **Explanation:** When you select "Shut down the computer" from the Windows "Shut Down" menu, the PC is completely powered down automatically instead of your being given the chance to do this manually, or, the opposite, you want this to happen and it isn't happening.
- **Diagnosis:** This is a power management feature that is built into Windows. In order to make use of it, you must have an [ATX](#) form factor motherboard, because ATX boards support the ability to have the PC turned off under software control. You must also have a board that supports advanced power management (APM) features. If the feature is not working then one of these conditions has been violated; if you want it to stop then you must disable the power management feature.

### Recommendation:

- If the system automatically powers down when you shut down Windows and you don't want this to happen, the easiest way to stop it is to disable all [power management features in the system BIOS](#).
- If you want automatic power-down to occur, make sure that you have an ATX system and that power management is not totally disabled in the system BIOS. You can tell the system BIOS to not activate its power-saving "standby" or "suspend" modes, if you wish; just don't totally disable all power management functions.

If you have power management enabled and an ATX system and power-off still does not work, try running an "Add new hardware" session in Windows (from the Control Panel) and have Windows search for new devices. It should find and enable the power management feature.

### The power doesn't come on

1. **No power from the wall socket:** Use a live power outlet. In rare cases, the power cable may be defective and may require replacement. Check the power cable on another working PC. Plug in a lamp or any other electric device to see if you have a live outlet.
2. **Incorrect voltage setting on the PSU:** Select the proper voltage setting (220-240V) on the back of the PSU. **WARNING:** If you have switched on the PC with the voltage set to 110-120V

ICT ITS1	Version:01	Page No.109
	Copyright: Ethiopia Federal TVET Agency	





and with a mains supply of 240V you may have blown your PSU beyond repair at worst or blown a fuse at best. Be careful!

3. **The front panel power switch's connector to the motherboard is not fixed correctly or has come off or is defective:** Check the motherboard manual and fix the lead (wires) from the front panel switch to the motherboard correctly. If there is still no power, try a different lead.
4. **The front panel power switch is defective:** Replace the switch. In case you do not want to get a replacement, one option is to use the reset button. The only problem with this is that to cut the A PSU with all its connectors power to the system in case of system hangs etc., you will have to switch off the power from the mains wall outlet rather than from the front panel.
5. **The power supply connections to the motherboard are not correct:** Check the power connections from the PSU to the motherboard. Refer to the motherboard manual and identify the correct connection points.
6. **Not identified; non-PSU related problem:** After attempting all the above, if the system still doesn't power up, it is time to look elsewhere. Disconnect all the drives and see if it is powering up. (*Note:* Pull out the power cord when removing or disconnecting something.) If the system is powering up, then start reconnecting the drives one by one to identify which is defective drive. If the system is not powering with all drives disconnected, remove the other adaptors one at a time and checking to see if it is powering up. Leave the video adaptor for the last. If you are able to isolate the problem to one of the adaptor cards, verify that the slot and the adaptor cards are compatible. Then try plugging it into a different slot and see if the system powers

If the system is still not powering up, then you either have a defective PSU or a defective motherboard. If there is a burnt smell, then most probably either one of them has been fried. Look for burn marks on the motherboard. Sometimes the PSU and motherboard may be incompatible. If the motherboard looks fine, replace the PSU, since it's cheaper! Check the relevant sections of this guide for troubleshooting hints for the other components.

### **The PC powers on after the second or third try**

The mostly likely problem is that the power\_ok (or power\_good) signal is sent before the power supply has stabilised. Get a better quality PSU. In modern PCs, the power switch is a logic device that tells the PSU to supply full power to the motherboard. The power\_ok signal tells the motherboard that the

<b>ICT ITS1</b>	Version:01	Page No.110
	Copyright: Ethiopia Federal TVET Agency	



power supply is available and stable. If the signal is sent too soon the motherboard does not recognize it and stays off to protect itself. This can happen in lower quality PSUs. Booting more than once is not recommended, and you will be better off getting a better PSU.

### **The PC powers on but nothing happens after that (no beep)**

1. This may be due to the addition of new hardware that is overtaxing the power supply. Remove the last hardware component installed and check again.
2. A defective hard disk or one that is not plugged in correctly: Check the power cable to the hard disk. Sometimes it may not be fully plugged in. Check the hard disk on another system.

### **The PC powers on, beeps and stops. No Power On Self Test (POST) messages.**

This may be a motherboard problem and not related to the PSU. Check the motherboard section of this guide.

### **The PC powers on and runs POST but there is no display**

This may be a display card problem and not related to the PSU. Check the display section of this guide.

### **There is a squealing/whistling/whining noise when the PC starts**

This could indicate either a problem with the fan, which has accumulated dirt over time, or one of the internal components of the PSU. Switch on the PC and listen carefully to confirm that it's the PSU fan and not the CPU fan or the hard disk. Usually, the noise will stop once the fan picks up speed, and you can ignore it temporarily. It's a good idea, however, to clean out the dirt around the PSU fan using a PC vacuum. This will increase the working life of the PSU fan as well as the PSU itself. If the fan stops working, the PSU will generate heat and cause more trouble. So a little prevention will save you a lot of headaches later. If the sound is not from the fan but from within the PSU itself, then you may be able to service it. A PSU has no 'user-serviceable' parts, and it's best left to a competent technician, although in most cases of component failure, you will have to replace the PSU.

### **The PC freezes or reboots suddenly**

1. This could indicate a failing PSU that is not supplying power correctly to the motherboard. You may be able to get the PSU serviced but in most cases you will be better off getting a new power supply.
2. This could be due to overheating of the PSU or CPU: If the PSU is overheating, the metal cabinet may be hot to touch or you might get a shock. Shut off immediately. Check if the PSU fan is

<b>ICT ITS1</b>	Version:01	Page No.111
	Copyright: Ethiopia Federal TVET Agency	



working, clean or replace the fan if not working or spinning very slowly. If it's a faulty PSU you may be able to service it. If the PSU seems normal it might be due to an overheating CPU.

<b>ICT ITS1</b>	Version:01	Page No.112
	Copyright: Ethiopia Federal TVET Agency	



## 5.1. Common Motherboard and BIOS Problems

**There is an apparent failure of the motherboard or a system device on the motherboard**

- **Explanation:** There is suspicion of a possible failure related to the motherboard. This can be a result of a specific message strongly implicating the motherboard in some sort of erratic system behaviour. It may also be the case that the motherboard probably isn't the problem, but that we want to rule it out as a possible cause. Since the motherboard is where all the other components meet and connect, a bad motherboard can affect virtually any other part of the PC. For this reason the motherboard must often be checked to ensure it is working properly, even if it is unlikely to be the cause of whatever is happening.
- **Diagnosis:** Outright motherboard failure is fairly rare in a new system, and extremely rare in a system that is already up and running. Usually, the problem is that the motherboard has been misconfigured or there is a failure with one or more of the components that connect to it. Getting a system in the mail that has a loose component or disconnected cable is very common. In fact, though, there are surprisingly large possible causes for what may appear to be a motherboard failure.

**Recommendation:** Follow the suggestions below to diagnose the possible failure of the motherboard. You will find a lot of possible causes listed below, since there are so many problems that can make it look like the motherboard is at fault. This part of the Troubleshooting Expert is referenced by a large number of other sections. For this reason, you may want to skip some of the steps below if you have already tried them elsewhere. Also, try to avoid the very difficult diagnostic steps--especially replacing the motherboard--until you have exhausted the other possibilities both here and elsewhere on the site:

- First of all, if you have just recently installed this motherboard, or performed upgrades or additions to the PC of any sort, [read this section](#), which contains items to check that may cause problems after working on the system unit.
- If the PC isn't booting at all, make sure you have at least the minimums in the machine required to make it work: processor, [a full bank of memory](#), video card, and a drive. Make sure that all of these are inserted correctly into the motherboard, especially the memory. Partially inserted memory modules can cause all sorts of bizarre behavior.

ICT ITS1	Version:01	Page No.113
	Copyright: Ethiopia Federal TVET Agency	



- Remove all optional devices from the motherboard, including expansion cards, external peripherals, etc. and see if the problem can be resolved.
- Double-check all the [motherboard jumper settings](#), carefully. Make sure they are all correct. In particular, check the processor type, bus speed, clock multiplier and voltage jumpers. Also make sure the CMOS clear and flash BIOS jumpers are in their normal, default operating positions.
- Reset all BIOS settings to [default, conservative values](#) to make sure an overly aggressive BIOS setting isn't causing the problem. Set all cache, memory and hard disk timing as slow as possible. Turn off BIOS shadowing and see if the problem goes away.
- [Double-check all connections to the motherboard.](#)
- [Check the inside of the case to see if any components seem to be overheating.](#)
- Inspect the motherboard physically. Check to make sure the board itself isn't cracked; if it is [look here](#). Make sure there are no broken pins or components on the board; if there are, you will have problems with whatever component of the PC uses that connection. Check for any socketed components that may be loose in their sockets, and push them gently but firmly back into the socket if this has happened.
- Make sure the keyboard is inserted correctly into the motherboard.
- A failed cache module or using the wrong type can cause motherboard problems. If you suspect it, [troubleshoot the secondary cache](#).
- An overheated processor can cause system problems. Try [troubleshooting the processor](#).
- [Troubleshoot the system memory](#). Memory problems are often mistaken for motherboard faults, especially on systems that don't have the protection of using memory [error detection](#).
- Try [troubleshooting the video card](#) or replacing it with another one, preferably a simple straight VGA card that is known to work from being in another system that functioned properly.
- If the power supply is older, or this is a cheap case, or you have added many new drives to a system with a weaker power supply (especially one that is less than 200W) then you may have a power supply problem. You may want to try replacing it.
- You may have a BIOS bug or other problem. Check your manufacturer's [technical support resources](#) for any known problems with your motherboard. Check on [USEnet](#) as well.

ICT ITS1	Version:01	Page No.114
	Copyright: Ethiopia Federal TVET Agency	



- Contact the technical support department of your system or motherboard manufacturer for additional troubleshooting information. If this is a new motherboard, you may want to consider [returning it for an exchange](#) if you have exhausted all other troubleshooting avenues.
- Some newer viruses, when activated, overwrite part of the BIOS code in systems that employ a flash BIOS. If the BIOS is corrupted, the system won't boot. [See here for ideas on recovering from this.](#)
- Try swapping the motherboard with another one and see if the problem resolves itself. If it does then the original motherboard is probably faulty, but it could just have been misconfigured or installed incorrectly.

## 2. There appears to be a failure related to the keyboard controller

**Explanation:** An error message or keyboard failure is implicating a possible failure of the [keyboard controller chip](#) on the motherboard.

**Diagnosis:** The keyboard controller chip can indeed develop a problem, although this is unusual. Using the wrong kind of keyboard, or a defective or incorrectly connected keyboard can also cause an apparent problem with the controller.

### Recommendation:

- [Troubleshoot the keyboard itself first.](#)
- Find the keyboard controller chip on the motherboard, and examine it. See if it looks damaged in any way. If it is, then it needs to be replaced (either that or the whole motherboard). You may be able to get a new controller chip, but you will have to contact your motherboard's technical support department.
- If the controller chip is socketed, check to see if it is fully in the socket. Gently but firmly push down on the chip. You may hear a "crackling" sound when you do this, which is fairly normal. This may resolve the problem.
- [Troubleshoot the motherboard.](#)

ICT ITS1	Version:01	Page No.115
	Copyright: Ethiopia Federal TVET Agency	



### **3.I have lost my BIOS password so I cannot start the system and/or get into the BIOS setup program**

**Explanation:** You entered a password into the BIOS setup program to control access to the system, and then forgot the password. If this a setup password, you will be unable to enter the BIOS setup program. If this is a startup or boot password, you will be unable to boot the system at all.

**Diagnosis:** For most people, using the BIOS passwords isn't a great idea, and this is the main reason why. If you do use a password, you should always record it in writing somewhere in case you need it later on. It can be hard to get around this sort of a problem, precisely because if there were an easy way to get around the password, it would have no value. In most cases you will have to clear the CMOS memory to erase the password.

#### **Recommendation:**

- If you haven't already, and if you can live without the machine for a day or so, wait and try to remember the password. This is the best solution, if you can remember it. :^)
- If your system has an AMI BIOS, try the default password, which is either "AMI" or "ami". This will not usually work, but is worth a try.
- If you cannot get into the BIOS program, your only remaining option is to try to clear the CMOS memory that holds BIOS settings. Included in this memory is the password, so this will let you get back into the PC. [See here for instructions on erasing the CMOS memory.](#)
- If it is a setup password that you are trying to get around, then you can at least boot the PC. It is possible in some systems that performing a flash BIOS upgrade will clear the CMOS memory and eliminate the password. I would not recommend trying this without getting confirmation from your motherboard vendor first, as doing flash BIOS upgrades in strange situations can theoretically be dangerous.

### **4. I need to clear the CMOS memory (due to a corrupted BIOS, lost password or other problem) but do not know how to do this**

<b>ICT ITS1</b>	Version:01	Page No.116
	Copyright: Ethiopia Federal TVET Agency	



**Explanation:** You need to clear the CMOS memory but aren't sure how to do this. It is sometimes necessary to clear the CMOS due to a lost BIOS password, corruption of the CMOS memory, or because you set the BIOS settings to values incompatible with your hardware and now you cannot boot the PC far enough to get into the settings and reset them (this rarely happens, fortunately).

**Diagnosis:** How easily you can clear the memory depends on the design of your motherboard. In some cases it can be easy to do but in other cases very difficult.

**Warning:** Erasing the CMOS memory will cause you to lose all settings in the BIOS. Make sure that you only do this if it is absolutely necessary. Basically, you should only do this if you can't get into the BIOS setup program due to hardware problems or a lost password.

**Recommendation:**

- Turn off the PC. Hold down the {Insert} key and then turn the PC on and wait for it to boot. On some PCs, this will clear and reset the CMOS memory for you. (On most PCs it will not work, so don't be discouraged.)
- Try the same thing with the {Delete} key. Again, it usually won't work.
- Look in your motherboard or system documentation for any evidence of a CMOS clear jumper. This is a [jumper on the motherboard](#) that can be used to clear the CMOS memory; many newer motherboards have them. Follow the instructions for its use as described in the documentation; usually this means opening the PC, changing the jumper to a special setting, and then booting the PC. The CMOS memory will be cleared. Then you power the PC down and put the jumper back to its previous position. If it doesn't work properly when you try it, [look here](#).
- If you do not have a CMOS clear jumper, your next option is to try disconnecting the CMOS battery. This is easy to do if the battery on the motherboard is removable or user-replaceable. If you see on the motherboard what looks like a flat round wristwatch or calculator battery in a holder, that's it. Some older motherboards use batteries that sit off the motherboard and connect with a wire. If the battery can be disconnected, then disconnect or remove it. Wait for about two

ICT ITS1	Version:01	Page No.117
	Copyright: Ethiopia Federal TVET Agency	





hours (you may need to vary the amount of time; if two hours isn't enough, try leaving it overnight) and then plug it back in, and the CMOS should be cleared and reset.

- On some systems, the CMOS battery is integrated within the BIOS chip. You *may* have success with removing the chip for a few minutes and then replacing it. Just be very careful to take anti-static precautions.
- Your motherboard may have a battery that is soldered to the motherboard. You may not see a battery on the motherboard at all; if this is the case then your motherboard probably uses a battery that is integrated into the real-time clock chip (or else, you weren't looking closely enough :^). Unfortunately, on a motherboard without a removable battery and with no CMOS clear jumper, clearing the CMOS memory is difficult to do. At this point you should contact your manufacturer for technical support.

**Warning:** Some people will recommend shorting the leads of the battery to clear the CMOS memory. I do not recommend this procedure, because shorting things on the motherboard is just generally a dangerous thing to do. Even removing the CMOS chip has the potential for problems. It really is best to contact the manufacturer of the motherboard or PC you are using in this situation.

## 5. My system has a CMOS clear jumper but when I use it, it doesn't seem to do anything

**Explanation:** You are following the directions to use the CMOS clear [jumper](#) on your motherboard, but the CMOS memory is not being cleared.

**Diagnosis:** The usual cause of this problem is neglecting to unplug the PC before attempting the procedure, or accidentally changing the wrong jumper. Some motherboards, particularly those using the ATX form factors, are supplying voltage to the motherboard even when it is off, and this is used as a "backup" for the CMOS memory when the battery is not working. (You're not supposed to be working inside the box with the power plugged in anyway, [remember?](#))

**Recommendation:**

ICT ITS1	Version:01	Page No.118
	Copyright: Ethiopia Federal TVET Agency	



- Unplug the PC, if it is plugged in.
- Make sure you are actually using the CMOS clear jumper and not a different one by mistake.
- [Troubleshoot the motherboard](#).

## 6. The CMOS battery is dead or dying

**Explanation:** The system is exhibiting behavior that implies that the [CMOS battery](#) is dead. This can include lost CMOS settings, the real-time clock losing time, or of course dead battery warnings at boot time.

**Diagnosis:** On an older PC, it is normal for the CMOS battery to fail at some point in time. They usually last for many years, with over five years being the norm, at least on older machines. Nobody knows for sure how newer machines will fare. On a new motherboard, this sort of message is a sign of a defect, although you shouldn't worry about it if it appears only the very first time the board is powered up. The solution is replacing the battery, and this can be an either easy or impossible task, depending on how much thought the motherboard manufacturer put into the design.

### Recommendation:

- If this is a new motherboard and you are getting an error saying that the CMOS memory was cleared, or that the battery is dead, try rebooting the machine and seeing if the message goes away. If it does, then the problem is probably resolved as long as it does not return.
- If this is a new installation and you are getting the error continuously, I would double-check any jumpers associated with the battery. Some motherboards have a jumper to select between using an internal and external battery. Also, [check out these common problems with new installations](#).
- Replace the CMOS battery. Note that on some motherboards it is not possible to replace the battery because it is integrated into the motherboard or a component such as the real-time clock. This is a bad design by engineers who lack vision, but is unfortunately all too common these days.
- If the battery cannot be replaced, or replacing it does not solve the problem, [troubleshoot the motherboard](#).

ICT ITS1	Version:01	Page No.119
	Copyright: Ethiopia Federal TVET Agency	



## 1. The CMOS battery is failing intermittently, indicating that it is losing power, or losing settings once in a while

**Explanation:** The [CMOS battery](#) is working sometimes, but is occasionally failing, causing loss of BIOS settings or error messages.

**Diagnosis:** This situation can be very annoying, and in some PCs can last for a very long time. It usually means that the CMOS battery voltage is getting low and that it needs to be replaced, especially if the problem is occurring with increasing frequency. It can also result from a bad connection to the motherboard.

### Recommendation:

- Double-check the battery connection to the motherboard. If the battery is removable, remove and reinsert it.
- Replace the CMOS battery, if this is possible with your motherboard.
- [Troubleshoot the motherboard](#).

## 2. The system clock is losing time or not keeping time accurately

**Explanation:** The system clock is not accurate; it loses a number of minutes each day, or stops incrementing the time when the system is turned off.

**Diagnosis:** The most common cause of this problem is the CMOS battery, which also backs up the date and time so it isn't lost when the machine is turned off. A weak CMOS battery can lead to problems with the real-time clock even if the battery isn't weak enough to cause the loss of BIOS settings. Some motherboards apparently disable the clock as a power-saving measure when the battery voltage gets low. Of course, sometimes the problem with the clock is simply that it is inaccurate. As motherboards get cheaper and cheaper in both price and construction, the quality of some of these components gets very questionable.

### Recommendation:

ICT ITS1	Version:01	Page No.120
	Copyright: Ethiopia Federal TVET Agency	



- [Troubleshoot the battery](#) to make sure that it is not causing the problem.
- [Troubleshoot the motherboard](#) to ensure that some other strange situation is not causing the problem.
- If the battery is not at fault, and you cannot find any problem with the motherboard, your remaining solutions are to replace the motherboard or to use software methods to compensate for the clock. There are utilities that will resynchronize the system clock with Internet time servers, and others that allow you to program them to adjust the system clock forward or backward a number of minutes each day, to keep the clock roughly accurate.

### 3.The BIOS settings in the CMOS memory have become corrupted or damaged

**Explanation:** The data stored in [CMOS memory](#) that controls the BIOS settings has become corrupted. This is usually seen in a warning or error message when the PC is booted, since the CMOS has a checksum value that is used to allow the BIOS to detect when the settings have become corrupted.

**Diagnosis:** The most common cause of this problem is the CMOS battery, which can cause erratic behavior if it is poorly connected or weak. It is also possible for other hardware or software problems to corrupt the CMOS memory, but this is unusual.

**Recommendation:** If you have created a [backup copy of your CMOS settings](#) then use them to restore the settings to the correct values. To find the problem itself:

- [Troubleshoot the battery](#) to make sure that it is not causing the problem.
- Make sure that you [scan the system for viruses](#). Viruses can corrupt the CMOS memory (although they cannot reside in it).
- [Troubleshoot the motherboard](#). Motherboard problems can sometimes (rarely) result in CMOS corruption.
- [Troubleshoot your power supply](#). A failing supply can lead to problems with the whole system, and especially motherboard components.

ICT ITS1	Version:01	Page No.121
	Copyright: Ethiopia Federal TVET Agency	



#### 4. can't figure out how to get into the BIOS setup program

**Explanation:** You need to get into the [BIOS setup program](#) to change some parameters, but don't know what key or keys must be pressed.

**Diagnosis:** On most modern systems, the key or key combination to press to enter the BIOS program is displayed on the screen when the system boots up, at the time when the BIOS is ready to enter Setup. Older systems often didn't specify the key(s) on the screen at boot time. Very old systems don't have a built-in setup program and one must be run from the floppy disk. Note that if your PC says to try a specific key combination and you try it, and it doesn't work, this could be due to a keyboard problem as well. Look for a keyboard error to come up on the screen.

**Recommendation:** Assuming that your PC is from about 1985 or later, it should have an integrated setup program (original XT computers used switches on the motherboard instead of a setup program.) Try the following key combinations, which I have listed approximately in order of popularity in today's system (there may be others as well):

- {Delete} (modern Award and AMI BIOSes)
- {F2} (modern Phoenix BIOSes)
- {Ctrl}+{Alt}+{Esc}
- {Ctrl}+{Esc}
- {Alt}+{Esc}
- {Ctrl}+{Alt}+{S}
- {Insert}
- {F1}
- Consult your system manufacturer for the key combination.

#### 5. I changed my BIOS settings but when I rebooted, they reappeared with the old values!

ICT ITS1	Version:01	Page No.122
	Copyright: Ethiopia Federal TVET Agency	



**Explanation:** You went into the BIOS setup program to make changes to the settings, and then rebooted the PC, but the changes were reversed to the old values when you rebooted the machine.

**Diagnosis:** You probably forgot to save the changes to the BIOS settings, or you selected the "Exit without saving" option instead of the "Save and exit" option in the setup program (which are, unfortunately, usually located right next to each other on the BIOS setup menu).

**Recommendation:**

- Make the changes again, and be sure to save them using the correct option in the setup program.
- If the changes again do not stick, [you might have a problem with your CMOS battery](#).
- [Troubleshoot the motherboard](#).

**6. I am having problems trying to flash my BIOS**

**Explanation:** "Flashing" the BIOS refers to [upgrading the BIOS program through software](#). This can allow you to quickly and easily increase the capabilities of your system, but if performed incorrectly

**Diagnosis:** It is extremely important to follow the manufacturer's instructions in detail when performing a flash BIOS upgrade. These upgrades are highly vendor-specific.

**Recommendation:**

- Read the instructions for performing the flash BIOS carefully. Some motherboards require a special jumper to be set on the motherboard in order to perform a flash BIOS upgrade. If this jumper is not set, the flash will not work.
- Perform the upgrade on a clean-booted system, from DOS (not any form of Windows) and with no drivers or special programs of any sort loaded.
- Do not be afraid to consult with the motherboard manufacturer's [technical support](#).
- If you improperly flash the BIOS, if the flashing is interrupted (by a power failure) or if you flash the wrong BIOS image, you may corrupt the BIOS chip to the point where the system will no longer boot.

ICT ITS1	Version:01	Page No.123
	Copyright: Ethiopia Federal TVET Agency	



## 1. I flashed my BIOS, and now the system is dead!

**Explanation:** The system BIOS is the key piece of software responsible for booting your PC. Incorrectly flashing it will often cause the PC to fail to boot.

**Diagnosis:** The cause is usually flashing the wrong BIOS image file into the BIOS chip. This happens more often than you'd think, since most flash programs are not intelligent and will allow you to program the wrong BIOS code into the chip. The BIOS corruption can also result from an error or interruption during any BIOS flashing procedure. Finally, some new viruses can corrupt the system BIOS.

### Recommendation:

- Some newer PCs come with a boot block feature that enables them to recover from a corrupted BIOS situation. If the BIOS code is whacked, a tiny built-in program will look on the floppy drive for the appropriate files to reload the BIOS. You should contact the manufacturer for instructions.
- You can usually purchase a replacement BIOS chip from the motherboard (not BIOS) manufacturer. Physically replacing the chip with another that has the right code will solve the problem.
- for other ideas on how to recover from this situation. **Warning:** Some of the procedures described on Wim's page are not for the faint of heart, especially hot-swapping BIOS chips, which has the (low, but non-zero) potential to cause injury or damage.

## 2. My hard disk spins down after a period of inactivity even though I disabled power management in the BIOS

**Explanation:** You have turned off [power management](#), but the hard disk still spins down after a period of inactivity.

**Diagnosis:** Sometimes the power management isn't really turned off; it's possible that more than one BIOS setting needs to be changed and they weren't all changed. There could be a BIOS bug as well.

### Recommendation:

ICT ITS1	Version:01	Page No.124
	Copyright: Ethiopia Federal TVET Agency	



- Go into the BIOS setup and double-check that power management really is turned off at a global level.
- If you are running Windows 95 OEM SR2, look in the Control Panel for an applet called "Power". Go into it, and uncheck the box that controls spinning down the hard disk.
- If the problem persists, it is possible that your BIOS has a bug. Contact your motherboard manufacturer for more information. There was definitely a bug in some Award BIOSes in late 1996 (a motherboard of mine had one). This sort of problem can normally be fixed with a [flash BIOS upgrade](#), if available.
- There could be a problem related to the hard disk, such as a loose cable, or a defect with the hard disk itself; double-check the hard disk connection.
- [Troubleshoot the motherboard](#).

### 3. I can't seem to enable ROM shadowing, or the system isn't working with ROM shadowing enabled

**Explanation:** You are trying to enable [ROM shadowing](#) in the system BIOS but the system is refusing to boot or behaving unstably when shadowing is turned on.

**Diagnosis:** Shadowing of the system BIOS works properly in *almost* every system. Shadowing of the video card usually works. Shadowing of adapter ROMs only works sometimes, depending on the system and on the peripheral. Turning on shadowing may reveal a general problem with the hardware, but usually if shadowing is the only thing causing the problem, the device you are trying to shadow simply isn't designed to work with it. For example, many adapters use both ROM and RAM in their address spaces, and shadowing will cause these to stop functioning altogether.

#### Recommendation:

- If the device you are trying to shadow is an expansion card, then the card may not allow shadowing. Consult your system documentation. If the device (as well as the system overall) works with shadowing disabled, it is generally better to just not worry about it, as the performance improvement is slight in this case anyway.

ICT ITS1	Version:01	Page No.125
	Copyright: Ethiopia Federal TVET Agency	





- If the video card will not allow shadowing, this may be a limitation of the video card, though this is uncommon. You may want to [diagnose the video card](#).
- A failure to shadow the system BIOS ROM can mean a motherboard problem. [Troubleshoot it](#).
- Any type of problem with shadowing can implicate a memory problem. You may want to [troubleshoot the system memory](#).

#### 4. The motherboard appears to be cracked

**Explanation:** The motherboard appears to have a crack in the board itself.

**Diagnosis:** Eek. This is not good. It's very rare for this to happen, actually. This most likely would have been caused by abuse, especially by being too forceful when inserting components. It may be caused by pressing too hard when inserting expansion cards, especially into a poorly-mounted motherboard. If the motherboard is new, it may have been a manufacturing defect. As for the board itself, if it is working OK, don't worry about the crack. Otherwise, it will need to be replaced; there is no practical way to repair damage of this sort.

#### Recommendation:

- If the board is new, and you suspect it may have been shipped with the crack, [return it for exchange](#).
- Examine the motherboard to determine if it is mounted into the case correctly. Consider adding additional plastic supports to brace the motherboard if it is flexing when pressure is applied to it.
- Be careful when inserting expansion cards and components into the motherboard.
- If the motherboard is not working, troubleshoot it to eliminate all other possible causes of the problem. If the motherboard is still causing problems, you should replace it and see if the problem goes away. If it does, the motherboard with the damage should be discarded.

#### 5. There is a component or pin broken on the motherboard

**Explanation:** A [component](#) is broken on the motherboard, or a pin that makes up one of the connectors or headers on the motherboard is broken.

ICT ITS1	Version:01	Page No.126
	Copyright: Ethiopia Federal TVET Agency	



**Diagnosis:** Depending on what the part is that is broken, this may or may not be a big problem. The only causes of broken components on a motherboard are manufacturing defect, abuse, or accidental damage. If the board itself is working OK, you may not need to do anything, but you may have difficulty upgrading or expanding the motherboard later on.

**Recommendation:**

- If the board is new, and you suspect it may have been shipped with the damage, [return it for exchange](#).
- If the motherboard is working OK, and if the component or pin damaged is a part of the system not currently being used, for example a second processor socket, or a SIMM socket not in use, or a second serial port you are not using, ignore the damage. Get a new motherboard when you are ready to upgrade the machine.
- If the motherboard (or the system as a whole) is not working, troubleshoot it to eliminate all other possible causes of the problem. If the motherboard is still causing problems, you should replace it and see if the problem goes away. If it does, the motherboard with the damage should be discarded.

**6. One of the pins on the motherboard is bent**

**Explanation:** One of the pins that makes up one of the connectors or headers on the motherboard is bent.

**Diagnosis:** This is usually a manufacturing defect, or is caused by rough handling or abuse of the motherboard. The pins are malleable and it is usually possible to correct the problem.

**Recommendation:** With the power to the motherboard disconnected, examine the bent pin carefully. Using a pair of needle-nose pliers, grasp the end of the pin firmly. Slowly, slowly, bend the pin back into the correct position.

**1. I cannot get the ZIF socket to loosen so I can remove the processor that is in it**

ICT ITS1	Version:01	Page No.127
	Copyright: Ethiopia Federal TVET Agency	



**Explanation:** The [ZIF socket](#) holding the processor seems to be "stuck" and cannot be loosened.

**Diagnosis:** This occurs quite frequently, especially with older motherboards. These boards have had the same processor sitting in them often for years and they can become rather "comfortable" in their present position. It is usually possible to extricate the processor, but you must be careful not to break the socket, or you can basically toss the motherboard (and maybe the CPU as well.)

**Recommendation:**

- First, realize that many sockets require you to pull the ZIF socket lever *out* slightly from the socket before trying to lift it up.
- Make sure nothing is physically obstructing the lever.
- The problem is usually that the lever gets stuck and won't push all the way up to loosen the processor. Try applying gentle but firm pressure. Try rocking the lever back and forth, gradually increasing the pressure against the resistance in the socket. Eventually the lever should move and the socket should pop open. Do not try to "push as hard as you can".
- If you cannot get the socket open, you will need to have the motherboard serviced.

**2. There is a suspected failure of the secondary (level 2) cache, or the system locks up or crashes after adding cache to the system**

**Explanation:** The [secondary cache](#) is suspected of failing. This may or may not have occurred after adding more cache to the system.

**Diagnosis:** Outright failure of the cache is unusual, especially on an existing system. The most common problem when adding cache to a system is using the wrong kind of cache, or adding it and not setting jumpers that the motherboard requires. You may also have accidentally jarred something else inside the PC.

**Recommendation:**

<b>ICT ITS1</b>	Version:01	Page No.128
	Copyright: Ethiopia Federal TVET Agency	



- Try [disabling the secondary cache in the BIOS setup](#). If the problem goes away, then the problem is most likely the cache or the motherboard.
- If you added more cache, make sure that you used the right sort of cache for your motherboard. Cache "COASt" modules may all look similar, but they are *not* universal. Consult your manufacturer.
- Ensure that the cache is inserted correctly into the board and is all the way into the socket or slot.
- Check the motherboard manual for any [jumpers](#) that you may be required to set or change when adding cache. Check in the BIOS setup for a BIOS setting that you may need to change (though this would be unusual).
- If you added cache, or recently worked inside the machine on something else, check out [this section that describes possible causes of problems after working inside the PC](#), some of which may be unrelated to what you were doing.
- If the system is acting unstable, [diagnose this here](#). It is possible that the problem is unrelated to the cache, even if it showed up after adding more cache to the system.
- After the PC has been on for a few minutes, touch the chips on the cache module. If they are very hot, this is a signal that the cache module itself may be bad. If you can't keep your finger on the chip for more than a couple of seconds without pain, the chips are hot! If you replace the module and the chips on the new module get hot also, the motherboard is implicated.
- Try to replace the cache module with another one. If the problem goes away, then the module was bad. Otherwise, you should [treat this as a motherboard problem](#).

### 3. I added more secondary cache to the system but I didn't see any improvement in performance

**Explanation:** You were told that adding more [secondary \(level 2\) cache](#) to the system would improve performance, but don't see it. The system seems the same as it did before.

**Diagnosis:** The truth is that especially if you already have 256 KB of cache, adding another 256 KB does not significantly impact on performance. The reason is that the original cache is already probably catching over 90% of memory requests, so there just isn't that much room for improvement. A 5%

ICT ITS1	Version:01	Page No.129
	Copyright: Ethiopia Federal TVET Agency	



improvement in overall performance is typical for a desktop user, and increases in speed of less than 10% are hard for most people to notice. Of course, this all assumes that your upgrade was performed correctly, and actually "took".

#### **Recommendation:**

- Make sure that the extra cache was recognized and is being used. When the system boots up, check to see how much cache it is reporting, and make sure it is the right amount.
- Double-check in your system manual to see if adding more cache requires any jumpers to be changed on the motherboard. Some do require this. Check in the BIOS setup for a BIOS setting that you may need to change (though this would be unusual).
- Run some benchmark programs and compare their results to before the upgrade. Some sort of improvement, even if minor, should be apparent.

#### **4. I put in a Pentium MMX OverDrive processor, and it works, but when I boot the system it disables the cache**

**Explanation:** When booting the motherboard with a Pentium with MMX OverDrive processor, the secondary cache is disabled or not functioning.

**Diagnosis:** This is often caused by a BIOS that is unable to recognize the OverDrive processor properly.

#### **Recommendation:**

- Ensure that the processor has been inserted correctly into the socket; [see this section for more troubleshooting of processors](#).
- Contact your motherboard manufacturer about a [BIOS upgrade](#).

#### **5. I have a motherboard that uses an Intel Triton II 430HX motherboard, which is supposed to support caching over 64 MB of RAM, but my PC still slows down with more than 64 MB**

<b>ICT ITS1</b>	Version:01	Page No.130
	Copyright: Ethiopia Federal TVET Agency	



**Explanation:** The system uses the [Intel Triton II 430HX](#) chipset in its motherboard, which is designed to allow caching of over 64 MB of memory. However, the system exhibits a slowdown when using more than 64 MB of RAM, similar to how a board that only caches a maximum of 64 MB would slow down in this situation.

**Diagnosis:** Unfortunately, once again, "el cheapo motherboard syndrome" is probably to blame. While the 430HX chipset supports caching up to 512 MB of RAM, it only does this if an *optional* second [tag RAM](#) chip is added to the motherboard, or if a larger single RAM chip is used in the first place. Some vendors do not add this chip, in order to save a buck or two. It is sometimes possible to correct this situation.

**Note:** How much actual cache you have doesn't affect directly how much memory you can cache. Even if you have 512 KB of cache, this doesn't mean you can cache more RAM than if you only had 256 KB. [See here for more on this little-known limitation.](#)

**Recommendation:**

- Check the motherboard and manual to figure out whether your board has the 11-bit tag RAM that is required for 512 MB of cached RAM. If it doesn't then [continue here for possible solutions](#).
- If you do have the tag RAM, then there is either a problem with the components, or something is misconfigured. [Troubleshoot the system memory](#) and [troubleshoot the cache](#) to make sure that there isn't some sort of problem that is responsible for the slowdown.
- [Troubleshoot the motherboard](#).

**6. My Triton II 430HX motherboard doesn't have enough tag RAM to support caching over 64 MB of RAM; is there anything that can be done to solve this?**

**Explanation:** The motherboard requires a second [tag RAM](#) chip to allow caching of over 64 MB of RAM with the [Intel 430HX chipset](#), and the motherboard doesn't have it.

ICT ITS1	Version:01	Page No.131
	Copyright: Ethiopia Federal TVET Agency	



**Diagnosis:** In some cases the tag RAM can be increased, but in others it cannot. It depends entirely on the design of the motherboard.

**Recommendation:** Consult your motherboard documentation or technical support options to see what your choices are. Your PC will probably fall into one of these categories:

- Some motherboards don't have the second tag RAM chip needed to cache over 64 MB of RAM, but they have a *socket* where the second chip can be added. If you have the socket, consult your manufacturer for the exact specifications of the chip required. Then purchase and install it, making sure to follow the manufacturer's instructions, and you should be all set. You may need to change a jumper on the motherboard. Cost is probably only a few dollars.
- Some motherboards accept a [COASt module](#) to expand the size of the cache that contains an extra tag RAM chip on it as well. If your motherboard is like this, then adding an extra 256 KB of cache to the motherboard will also add the extra tag RAM and will let you cache over 64 MB. This situation is what sometimes makes people think that it is the adding of extra cache that enables more memory to be cached. In fact, it is the extra tag RAM chip on the module, not the cache chips themselves.

**Note:** Not all cache modules have tag RAM on them, and not all cache modules work with all motherboards. Make sure you find out exactly what you are buying, and if it will work with your board.

- If you don't have a socket and you can't add tag RAM via a cache module, you are basically out of luck. You will have to either accept slower performance when going over 64 MB of RAM, use less memory, or replace your motherboard. If the motherboard was just bought you may be able to [return it for exchange or refund](#).

## 1.Updating ESCD...

**Explanation:** ESCD stands for "extended system configuration data", and is where [resource information is stored](#) on a system that uses [Plug and Play](#). This message is displayed when the system

ICT ITS1	Version:01	Page No.132
	Copyright: Ethiopia Federal TVET Agency	



detects a change in the hardware configuration and therefore updates the Plug and Play information that it has stored. In some systems it may appear every time the PC is booted, however, even if the hardware configuration has not changed.

**Diagnosis:** Depending on the circumstances, this message may indicate an error or a normal operating condition.

**Recommendation:**

- If the system displays "Updating ESCD... Success" after adding or removing hardware on the next boot-up only, then this is normal for many BIOSes, and no action is required.
- If the system displays the message every time the PC boots, then there may be a conflict between the BIOS and the operating system. The ESCD information is managed by both the BIOS and by Windows 95 (or other Plug and Play operating system) to allow for Plug and Play resource allocation. However, some BIOSes record hardware configuration information in a way that is different from how Windows 95 does it. When this happens, each time Windows 95 is started it will change the ESCD area back to the way it expects it to be. When you reboot your system, the BIOS will see this change made by Windows 95 and change the data back to the way *it* likes it. This back-and-forth will continue to happen each time the system is booted. It doesn't generally cause any problems other than displaying the "Updating ESCD" message every time the system is started up. You can contact your system or motherboard manufacturer about a possible BIOS upgrade to correct this situation. Other than it being annoying to some to see this message every time the PC boots, the system should continue to work without any problems.
- If the system displays "Updating ESCD..." and then hangs up the boot process, either with or without displaying "Success", then there is a problem with updating the extended system configuration data. This is probably a problem with an expansion card, especially if you just added one to the machine. It could also be a problem with the motherboard. You should [troubleshoot this as an expansion card problem](#), and if this fails, [troubleshoot the motherboard](#).

ICT ITS1	Version:01	Page No.133
	Copyright: Ethiopia Federal TVET Agency	





## 2. I have a PCI expansion card or video card that is supposed to support bus mastering, but I can't get bus mastering to work

**Explanation:** PCI bus mastering is supposed to be supported by a video or expansion card, but is not working properly. (Note that [problems with IDE hard disk bus mastering is discussed in this section](#), not here.)

**Diagnosis:** Bus mastering problems are generally hard to diagnose, and often depend a great deal on the specific card. General problems with bus mastering can be related to the motherboard or BIOS settings.

### Recommendation:

- Consult the documentation for the peripheral card *carefully*. Usually the answer to the problem will be there somewhere.
- Search your motherboard documentation for any hints as to whether all of your PCI slots support bus mastering, or only some of them. Some early and/or cheaper motherboards only supported bus mastering in some of their PCI slots, but not all of them.
- Double-check all BIOS settings that are in the [PCI / PnP settings group](#). Make sure that you are not disabling bus mastering, or assigning resources incorrectly to only ISA legacy cards.
- You may have a [resource conflict](#) associated with the card..
- [Troubleshoot the expansion card](#).
- [Troubleshoot the motherboard](#).

## 3. I have a suspected system failure related generally to expansion cards in the system

**Explanation:** A problem condition with the system overall is arising that implies a possible problem related to one or more of the expansion cards in the system. (This means a problem with the system caused by expansion cards, not a problem with a specific card in a system that otherwise works; [look here for that](#).) This typically means an error message or a failure of the system to boot.

ICT ITS1	Version:01	Page No.134
	Copyright: Ethiopia Federal TVET Agency	



**Diagnosis:** The wide availability of many different types of expansion cards means that the chances of a conflict between two of them, or between them and the system, are significant. Resource conflicts are the most likely problem.

**Recommendation:**

- Make sure all the cards are securely inserted into the system. Very long cards, especially those that use the [VESA local bus](#), can sometimes come partially loose, causing strange results.
- Make sure that there are no [physical problems with the motherboard or internal connections](#).
- Disable all [shadowing of expansion adapter ROMs](#) and see if that fixes the problem.
- Remove all unnecessary expansion cards (basically, everything but the video card) and see if the problem goes away. If it does, the problem is probably one of the expansion cards you removed. If not, your problem lies elsewhere. Try to isolate the problem by inserting one expansion card at a time back into the system and seeing which one triggers the problem.
- Since the most likely cause of the problem is a resource conflict, [look here for ideas on resolving the conflict](#).
- [Troubleshoot the motherboard](#).

**4. I have a specific expansion card that appears to be problematic**

**Explanation:** A problem is suspected with a particular expansion card. (This means a problem with the card itself, not a problem with the overall system caused by one or more expansion cards; [look here for that](#).) This is typically manifested through an error message, such as a ROM checksum error or I/O parity error.

**Diagnosis:** Most of the problems with specific expansion cards depend entirely on the nature of the card. I can only provide some general pointers here.

**Recommendation:**

- Make sure all the cards are securely inserted into the system. Very long cards, especially those that use the [VESA local bus](#), can sometimes come partially loose, causing strange results.

ICT ITS1	Version:01	Page No.135
	Copyright: Ethiopia Federal TVET Agency	



- Make sure that there are no [physical problems with the motherboard or internal connections](#).
- Make sure that the connections, jumpers and any software drivers associated with this card are correct.
- If this card has its own BIOS ROM, make sure that the shadowing of that segment of ROM address space is not enabled, [as this can cause problems](#). (Shadowing will work with many cards, but won't work with some of them.)
- Remove any other expansion cards in the system and see if that affects the problem. If it does, then either the other card was causing the difficulty, or there is some sort of a resource conflict.
- [Check for resource conflicts](#) in general.
- Try the card in a different slot and see if it works. This is especially true of PCI cards, which will try to use different IRQ lines depending on which slot they are placed into. By changing the slot you may as a side-effect eliminate a resource conflict that was actually causing the problem.
- If the card is a video card, [troubleshoot it here](#).

## 5. I think I have a resource conflict in my system; what can I do about this?

**Explanation:** It is suspected that the system may have a [resource conflict](#). This means that two different devices are both trying to use a system resource like an interrupt request line, DMA channel or I/O address. The two devices will conflict and cause either one or both to malfunction. [A list of typical symptoms of resource conflicts can be found here](#).

**Diagnosis:** Resource conflicts are one of the most common problems with PCs, especially with those who upgrade or add equipment to their PCs. Since the ancient architecture of the PC has resulted in a great variety of internal devices and expansion cards having to share a limited amount of resources, devices will often "step on each others' toes". The problem is almost always misconfiguration; in rare cases you will not be able to use two devices in the same system if they cannot find a way to cooperate by configuring themselves to use available resources.

**Recommendation:**

ICT ITS1	Version:01	Page No.136
	Copyright: Ethiopia Federal TVET Agency	



- [Read this section of the Reference Guide](#), which contains much more information on resource conflicts.
- Do not try to "share" resources. Some people will say that this is possible to do, and technically it is, but it is a headache that is not worth dealing with in my opinion. Windows 95 is particularly unforgiving about trying to share resources.
- If you suspect a conflict with a specific device, and you are running Windows 95, go into the Device Manager. Click on the device with the problem (which may show with a yellow exclamation-mark-in-a-circle next to it) and select "Properties". Click on the "Resources" tab and the system will often tell you what the conflict is.
- Sometimes, folks think they have a resource conflict because the Windows 95 Device Manager shows a PCI device on the same IRQ as another device called "IRQ Holder for PCI Steering". This is in fact not a resource conflict; IRQ steering is a feature of Windows 95 that is designed to help *avoid* resource conflicts. If you think you have a resource conflict you may indeed have one, but this isn't it.
- Use a [diagnostic tool](#) such as Norton Diagnostics. There is a test in this package that looks for the IRQ usage of various devices and will sometimes highlight conflicts (though it is not perfect by any means).
- Catalog the resource usage of all of the devices in your PC. This is the best way to determine what resources are being used by what. You may find [the device resource summary sheet I have included here](#) to be helpful with this. If you find any devices that are trying to use the same resources, try to change the configuration of one of them.
- Check [resource-related BIOS settings](#) to ensure that they are correct.
- Watch out for PCI devices using IRQs. The PCI bus [uses its own interrupt scheme](#) but PCI devices also "map" to regular IRQs when needed. Many PCI video cards, for example, use an IRQ, typically 9, 10, 11 or 12. Make sure that this does not cause any conflicts with other devices.
- If you are using IRQ9 for any device, make sure you are not using IRQ2 on any other device. [They are the same interrupt line](#).
- If you are trying to use the COM1 port and the COM3 port at the same time, or the COM2 port and the COM4 at the same time, you will run into a conflict if you leave these ports at their default IRQ settings. [Each of these two pairs uses the same IRQ number](#). To use COM1 with COM3,

ICT ITS1	Version:01	Page No.137
	Copyright: Ethiopia Federal TVET Agency	



or COM2 with COM4, you must change the IRQ number that one of the pair is using so that it does not conflict with the other.

- If you add a modem to your system, and you have a built in COM2 port (which most do) you will see a conflict unless you change the modem's settings, because most of them default to use COM2. If you just change the modem from COM2 to COM4, then the problem above will result unless you also change the IRQ of the modem to another number.
- If you are using a sound card and a second parallel port, you will probably have a conflict, because both devices try to use IRQ5 by default. One or the other must be changed. (Also [watch out for the first parallel port accidentally being set to IRQ5](#)).
- If you are using a secondary IDE controller, then IRQ number 15 is normally used by that controller and cannot be used by other devices.
- DMA conflicts are commonly caused when [enabling ECP parallel ports](#). They use a DMA channel while other modes of operation of the parallel port do not.
- If you are using a network card, beware of I/O address conflicts. Many network cards use [a full 32 bytes of I/O address space](#), and can conflict with other devices. They also sometimes try to use IRQs that are commonly used by other system devices such as video cards or hard disk controllers.

## 6. My system is reporting that it has a "static resource conflict"

**Explanation:** On rare occasions, some motherboards may produce an error at boot time saying that they have detected a "static resource conflict". This is a result of the [Plug and Play](#) feature of the BIOS and is saying that more than one device is trying to use the same Plug and Play system resource. Usually this will not occur because the BIOS will adjust resource allocations to prevent a conflict.

**Diagnosis:** The most usual cause of this problem is certain cards that designate their resource usage in a strange way. Without getting into too many details, some peripherals such as the Pro Audio Spectrum will allocate an I/O address in two different ways. It is the same resource, but the BIOS becomes confused and thinks that there is a conflict. In other cases, the BIOS thinks there is another kind of conflict when there isn't. The BIOS usually needs to be reset to avoid this situation recurring.

ICT ITS1	Version:01	Page No.138
	Copyright: Ethiopia Federal TVET Agency	



## Recommendation:

- Attempt to discern, if possible, whether or not you really have a [resource conflict](#). If you do, then resolve this situation.
- Try to reboot the system to see if this makes the problem go away.
- Remove all expansion cards from the system and reboot the PC. This may make the problem go away so you can boot the machine. Then re-insert the cards and see if the message goes away.
- If you cannot get the message to clear, you will have to [clear the CMOS memory](#).

<b>ICT ITS1</b>	Version:01	Page No.139
	Copyright: Ethiopia Federal TVET Agency	



Self Check 5

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Write the answer briefly**

1. The PC's internal power supply appears not to work at all. The system will not turn on and the power supply itself appears to be dead. Write Diagnosis?
  
2. "Flashing" the BIOS refers to [upgrading the BIOS program through software](#). This can allow you to quickly and easily increase the capabilities of your system, but if performed incorrectly . Write Diagnosis?

**Note: Satisfactory rating –1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.140
	Copyright: Ethiopia Federal TVET Agency	



## Information Sheet – 6

### Using the operating system and third-party diagnostic tools

#### 6.1. Using diagnostic tools

Each computer system has built into it a range of tools to help the user determine its 'status'. By 'status' we mean that they help determine if the system is working correctly or not. If a system is not working correctly, diagnostic tools can provide information vital to solving the problem. The most common types of computer problems will be found during these processes:

- booting the computer
- loading the operating system
- manually checking the system.

Diagnostic tools are available at each of these stages and are outlined in the following sections. These tools provide the foundation of any troubleshooting that involves the malfunctioning of a computer.

**IMPORTANT:** You will be directed to use a number of diagnostic and configuration tools to gather information about your system. Changing **any** of the settings using these tools may cause your computer to malfunction. If you are in any doubt about the use of a particular tool, contact your supervising teacher.

You may also be required to make system changes to solve problems identified by the diagnostics. Again, the types of changes required, if incorrectly applied, may cause your computer to malfunction. If you are in doubt about how to proceed with system modifications, consult your supervisor.

#### Booting the computer

Booting a computer system involves turning the machine on, checking that power LEDs come on and that the screen reflects the expected activity of the system start up procedure. In a PC system, part of this procedure is the Power On Self Test or POST diagnostic tool. The POST diagnostic tool is built in to the system and starts automatically when the system is turned on.

ICT ITS1	Version:01	Page No.141
	Copyright: Ethiopia Federal TVET Agency	





Any failure related to a major component, such as motherboard, video, keyboard or drive failures, will be detected during the POST phase of a computer system. The total failure of a major hardware component is easily detected. Less crucial devices that fail will normally be detected by the operating system as it loads and are dealt with in the next section.

Most hardware systems such as computers and printers have a POST tool to check that their major components are working properly.

### Power On Self Test (POST) diagnostic tool

During the PC computer system’s loading phase, each of the main components are tested. The failure of any one of these systems would impair the computer’s ability to operate. Such critical devices include the graphics card, motherboard resources, drives and Input/Output (I/O) interfaces such as keyboard and graphics (video cards).



**Figure 1:** Power On Self Test (POST) diagnostic tool

On a PC based system, this provides feedback on the screen about the type of video card detected, the type and speed of the processor detected, the type and number of drives detected, as well as the amount of Random Access Memory (RAM) detected. It checks the presence of peripheral devices such as keyboard and mouse devices. It also internally tests the correct performance of many motherboard components.



Any failures at this level may result in an error message on the screen, or may be heard as a series of coded 'beeps'. The beep codes are often unique to a motherboard model and should be interpreted by information found on the motherboard manufacturer's website.

The POST screen will only briefly appear at the start of the booting process. The CPU's type and speed will be listed here with other device information. On many systems, pressing the **Pause** key during this process will freeze the screen, and the **space bar** key releases it. If you cannot pause the screen, check with your supervisor or teacher as it may take several restarts to view the information fully. If you must reset the computer, be careful to do so by pressing the reset button before the operating system begins to load, as this will prevent it from recording failed loading attempts.

To view the systems detected configuration more fully, examine the system Setup or **CMOS** tool. Some references may prefer to use the term **BIOS** in place of the term CMOS. They refer to the same tool. To enter this tool, users are normally required to press a key or key combination such as the **DEL** (Delete) key or **Shift + F10** during the POST sequence. Because these settings effect the operation of the PC, many companies password protect this tool so unauthorised users cannot access this area.

The Setup or CMOS tool for your PC holds the configuration of your computer. It lists how much memory the system has, how many drives are detected and which drive it should load the operating system from. It will also have configuration options for a range of other items such as power management and I/O interfaces, just to name a few.

The motherboard manual that came with the PC holds information about the CMOS tool and its use.

At this level, the tool is simply used to determine that the system has detected its elementary components such as RAM, HDDs, FDD, etc. The CMOS settings should reflect the known configuration of the PC. Normally the IDE drives should be set to 'AUTO' which stands for Automatic Detection. Any errors such as RAM or drives not being recognised by the system should be recorded and reported to a supervising technical support person.

The default or factory settings can normally be restored by choosing the relevant menu option. **When you exit the CMOS, exit without saving your changes, unless you have deliberately changed a setting.** This prevents accidental changes from occurring.

ICT ITS1	Version:01	Page No.143
	Copyright: Ethiopia Federal TVET Agency	



For a Macintosh system, when you boot the PC will either show a happy face and load, or show a sad face and refuse to load.

Fixing faults detected here, on either a PC or Mac system, may require the case to be opened and can effect the warranty of the computer. It must be authorised by your manager who will refer it to an appropriate technical person.

## Loading the operating system

Once the POST sequence has been completed, the system then looks for a boot device as the CMOS configuration dictates. From here the computer begins to load the series of services or programs that together form what is called the operating system (OS). Normally the operating system's name and version (or service pack number) will be displayed during this process.

## Log files and OS booting tools

Common failures at this point may relate to the failure of minor hardware devices or incorrect configuration of devices that are physically OK. Any services or devices that fail to load are usually noted in a log file by the operating system. This file can then be examined at a later time to help determine what went wrong. Most Windows and Unix systems create log files during the loading process. These log files provide details that will alert you to errors. Many of the system log entries are fully explained in the operating system's documentation or the support section of their Internet site.

## Exercise

The following screen is from the system log of a Windows XP system.

Type	Date	Time	Source	Category	Event
Information	12/08/2004	5:04:55 PM	RemoteAccess	None	20155
Information	12/08/2004	4:59:38 PM	RemoteAccess	None	2015E
Warning	12/08/2004	1:37:58 PM	Dhcp	None	1007
Information	12/08/2004	1:36:50 PM	eventlog	None	6005
Information	12/08/2004	1:36:50 PM	eventlog	None	6009
Information	12/08/2004	1:02:46 PM	eventlog	None	6006

Figure 2: System Log of a Windows XP system

ICT ITS1	Version:01	Page No.144
	Copyright: Ethiopia Federal TVET Agency	



Examine entries in the log to determine which (if any) represent possible errors in the booting process. Each entry has an Event ID number that can be searched for in the Microsoft Knowledge Base. Search the Knowledge Base at <http://support.microsoft.com> for Event ID 1007 and determine the nature of the event warning.

If the system failure is so bad that the operating system fails before its loading process is complete, most systems provide tools that allow the computer to boot in restricted or 'Safe' modes, or alternatively provide emergency recovery disks. Using these options, the system then boots with a reduced set of services, allowing you to examine boot logs or device management tools to help detect problems.

Entries in the system log may require further research to explain their full meaning. Most operating system companies provide documentation on their website to assist in the interpretation of log file messages. For Windows 2000/XP, Microsoft's Knowledge Base website has many articles about different Event Viewer messages.

## Manually checking the system

### Device management tools

Most operating systems now work with the concept of 'Plug and Play' devices. This simply means that when a new device is installed, the system will automatically detect it and install the most appropriate software drivers for it.

A driver is a small piece of software written for a specific device. To make life simpler, many standard drivers are built into operating systems so they automatically work when installed. However, special features of that particular device model may only be available if the manufacturer's device driver is installed.

<b>ICT ITS1</b>	Version:01	Page No.145
	Copyright: Ethiopia Federal TVET Agency	

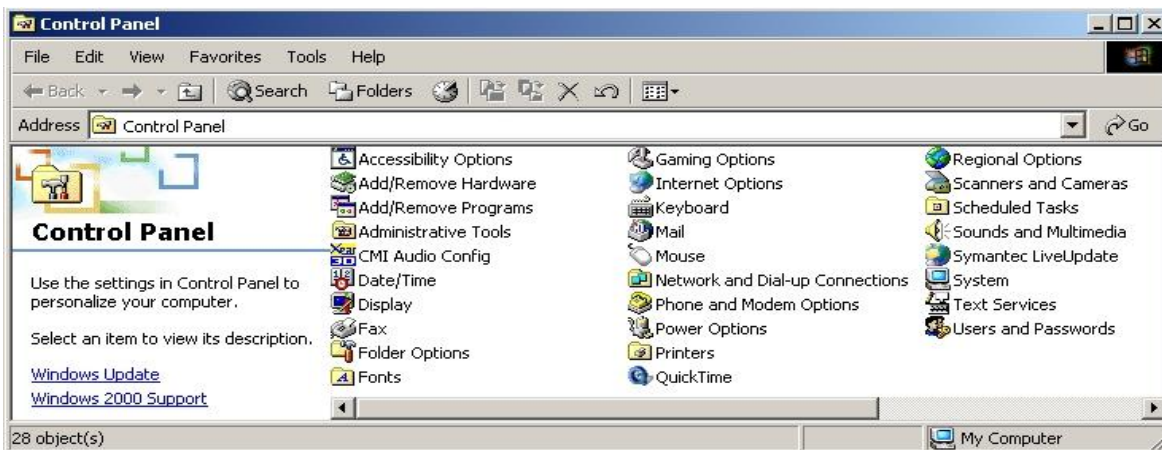


All current PC and Mac operating systems provide you with tools to look at the devices installed on your computer. In this context, a 'tool' is a small program that is designed to perform a limited, specialised role — such as providing information about a hardware device.

In a graphical user interface (GUI), which Windows, Macintosh and most Unix-based operating systems have, the tool may be represented by an icon. It may also form the properties of an object represented on the desktop, such as 'My Computer'.

In a text-based system, which Unix and Windows based systems also have, the tool may be in the form of a specific command related to a specific device.

Examples of tools are shown in the following screen shot.



**Figure 3:** Configuration tools

Device Management tools provide you with information and configuration options for devices attached to your system. They should provide you with a list of devices attached to your system and information about their status.

In a PC system these tools should also list the resources that devices use, such as an Interrupt (IRQ), Input/Output (I/O) memory range and Direct Memory Access (DMA) channel, etc. In a Mac system, the resource allocation for devices is automatic. Device Management tools may provide information about the software driver that was installed to manage the device.

<b>ICT ITS1</b>	Version:01	Page No.146
	Copyright: Ethiopia Federal TVET Agency	



In some operating systems, many different tools may be required to find this information. In other operating systems, this information may all be available from one tool.

## Management of hard disk drives

Hard disk drives are a vital part of any computer system. They retain data saved as files and can have a directory or folder system to organise files into a logical system. The constant writing, modifying and deleting files may cause errors from time to time. These errors often relate to file processes, such as saving a file that has been interrupted before it could be completed. This interruption could be caused by a power outage, application crash or shutting down a system incorrectly.

### Checking the file system

Each operating system provides you with standard tools to check the integrity of the file system. While different operating systems may support a range of different file systems, the basics remain the same. There is some master record of what files are on a drive and where those files can be found. This is called the **File Allocation Table (FAT)**. The FAT holds the list of files contained on the drive and the address of the first block where that file is stored. It is effectively a 'table of contents' to the disk drive.

Checking the integrity of the file system involves matching the FAT against the drive's contents. Should this become damaged, or incorrect, the results for your data could be devastating.

### Checking the drive

Your operating system may also provide you with an option, or separate tool, to check the actual integrity of the drive. By this we are referring to a process where the actual data blocks on the drive are checked to ensure that they store data correctly. Originally this is also done when you format the drive, which is why it can take so long to format large hard disk drives.

### Defragging the drive

It is also possible that your drive becomes 'messy' which is known as **fragmentation**.

ICT ITS1	Version:01	Page No.147
	Copyright: Ethiopia Federal TVET Agency	



Imagine your drive as a book, where information (or data) saved as files is written on the first available page (or block). When saving is complete, the file name and the page it starts on are entered into the 'Contents' page (or File allocation Table) of the book. The next file saved will take the next available page and so on.

However, when we wish to add more data to the first file we may require more than one page to hold the additional information. It can't be stored on the next page as it is already used by another file. So the next available blank page is used and we must link the first page of the file to the page number that is the second page of the file.

Having a file spread over a series of 'non-contiguous' blocks slows the reading and writing processes. The term 'non-contiguous blocks' simply means a series of blocks which are not stored next to one another. This is called fragmentation.

The process of **de-fragmentation** refers to a tool which tries to rearrange files into contiguous blocks to improve the performance of the file system. It can be dangerous as any interruption to this process may result in data loss and corruption. Always ensure that a backup exists for a drive before running a tool to de-fragment your disk.

<b>ICT ITS1</b>	Version:01	Page No.148
	Copyright: Ethiopia Federal TVET Agency	



Self Check 6

Written Test

Name: \_\_\_\_\_

Date: \_\_\_\_\_

*Instruction:* Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

**I. Fill the blank**

1. \_\_\_\_\_ involves turning the machine on, checking that power LEDs come on and that the screen reflects the expected activity of the system start up procedure.
2. \_\_\_\_\_ is built in to the system and starts automatically when the system is turned on.

**Note: Satisfactory rating –1 points**

**Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

**Answer Sheet**

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

<b>ICT ITS1</b>	Version:01	Page No.149
	Copyright: Ethiopia Federal TVET Agency	





## Reference

1. <https://training.gov.au/Training/Details/ICTSAS506>
2. [web1.keira-h.schools.nsw.edu.au/faculties/IT](http://web1.keira-h.schools.nsw.edu.au/faculties/IT)

<b>ICT ITS1</b>	Version:01	Page No.150
	Copyright: Ethiopia Federal TVET Agency	