INFORMATION TECHNOLOGY

SUPPORT SERVICE

Level I

Learning Guide #37

Unit of Competence: Maintain Equipment and Software Inventory and Documentation

Module Title: Maintaining Equipment and Software Inventory and Documentation

LG Code: ICT ITS1 M05 LO2 –LG-37

TTLM Code: ICT ITS1 M05 TTLM 1019v1

LO2: Store Technical Documentation

Instruction sheet	Learning Guide 37

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

- store software, hardware and equipment not in use
- Storing securely technical documentation.
- Accessing and disseminating technical documentation as required by clients.

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 –

- Take action to ensure software, hardware and equipment not in use, stored in a manner as recommended by technical manuals.
- Store securely technical documentation.
- Access and disseminate technical documentation as required by clients.

Learning Activities

1. 1Read 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 and Sheet 3” in page , 7 and 12 respectively.
4. Accomplish the “Self-check 1, Self-check 2 and Self-check 3” in page 5, 8 and 11 respectively
5. If you earned a satisfactory evaluation from the “Self-check” proceed to “Operation Sheet 1 for 3 information sheet ” in page 15
6. Do the “LAP test” in page 16

*Your teacher will evaluate your output either satisfactory or unsatisfactory. If Unsatisfactory, your teacher shall advice you on additional work. But if satisfactory you can proceed to the next topic.

Information Sheet – 1	Store Software, Hardware and equipment not in use

1.1 storage

1.1.1 Storage of Basics

Equipment not being used should be stored. It may be **new hardware and software** in boxes, or loose parts, or sensitive materials that need to be stored securely until installed or needed. Valuable items such as memory chips or original software copies may need to be locked in a safe.

An IT store can hold new hardware, spare parts, repaired equipment, extra copies of software, daily and weekly backup copies of files as well as memory chips. It can also hold redundant devices such as printers, modems, cables and tools. While the IT department may also keep contracts, licences and other documents, some companies prefer to keep such documentation in their Legal department (if there is one).

IT equipment is often delicate and expensive. The environment for IT hardware and software storage should be:

- Lockable
- Dust-free
- Static-resistant
- Safe from water and humidity
- Well ventilated and light
- At a constant temperature
- Separated from other perishable stores.

1.2 Guidance from technical manuals

Most IT equipment is fragile/easily broken and should be handled with care it can be damaged if not packed correctly in storage. The technical manual that companies equipment will often advise on packing and storage.

It is also advisable to access the website of the manufacturer. Often they update information about equipment on their website, or add additional information on packing and disposing of computer consumables and equipment.

Information from technical manuals needs to be recorded in the inventory for all stock (in storage or being used) such as the expected lifetime of the product. Printer manuals, for instance, will state how many pages can be printed before the toner cartridge or developer needs replacing. Packed and unopened toner cartridges can be kept for quite some time, but developer has a more limited shelf life.

1.3 Storing components, software originals and documentation

All information about storing components can also usually be found in technical manuals. Generally, sensitive components will be stored as follows.

1.3.1 Memory chips

Each memory chip should be placed in a foam-protected, anti-static bag. Each bag is then placed in an individual box or in a larger box that will have separate slots for each chip. Memory was once very expensive and always stored in a safe. However, as the cost of memory has fallen, memory is often stored alongside other components.

1.3.2 Expansion cards, motherboards and other spares

Expansion cards also must be placed in anti-static bags and each bag then placed in an individual box or in a larger box that will have separate slots for each card. This box is then stored in the storeroom, with care taken, if the box is cardboard, not to place other

equipment on top of it. Motherboards and other spares should be kept in boxing so that they are not stacked on one another and also to avoid dust building up.

1.3.3 CD-ROM drives and hard disks

CD-ROM drives are stored in stacks on a shelf in the storeroom. An obvious caution to take is that the stack is not too high, as it may topple over. Hard disks should be placed in foam-protected anti-static bags. Each hard disk needs to be stored in an individual box. The boxes can be placed on top of each other in stacks (again, not too high).

1.3.4 Software originals

When an organisation purchases software, copies need to be made of all disks. Installation of the software should be carried out with the copied disks and *not* the original. This ensures the security of the original disks, and if there are any problems with the copied disks another copy can be made.

The original disks need to be stored in a secure place such as a safe and preferably off site as a form of assurance against any problems within the building, such as flooding from heavy rain or fire damage.

Self Check 1	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. One of the following is not safe environment for IT hardware and software storage s
   A. lockable and dust-free
   B. safe from water and humidity
   C. well ventilated and lit
   D. at a constant temperature
   E. All
2. Equipment not being used should be stored.
   A. True B. False
3. Store securely hardware and software equipment is very important
   A. True B. False
4. The technical manual that companies equipment will often advise on packing and Storage any place.
   A . True B. False
5. IT equipment is often delicate and expensive
   A . True B. False

Note: Satisfactory rating - 3 and 5 points Unsatisfactory - below 3 and 5 points
You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Short Answer Questions

Information Sheet – 2	Store securely technical documentation.

2.1 Documentation

Documentation, including manuals that come with hardware and software, needs to be stored correctly. Some manuals may need to be kept with the relevant computers if they are used regularly. Generally, manuals are kept in a storeroom or IT library (which may be in the same place). They are only used at times of installation and later on for troubleshooting. They should be indexed in the inventory and labelled clearly on shelves or in cabinets. Documentation such as licensing should be recorded and stored in a safe area, such as a locked filing cabinet. As mentioned, in some larger companies, it may be kept the legal department or in a safe

2.2 Technical documents

Technical information may need to be available throughout the organisation. Some documents will have limited access, some may be found on the open shelves in the IT work area, and others kept in client's offices. In a highly developed business, images of documents can be online via the IT network.

2.3 Document control

Working in an IT reference section you might be expected to handle changes to technical users' manuals written by staff in your own IT department. Document control includes withdrawing old versions, disposing of them and issuing updated copies. To do this job efficiently, your records inventory must show who holds copies.

2.4 Levels of access and the currency of documents- General access

IT documentation can hold details of flow charts, program code, and technical reports, wiring plans, testing results, measurements and system analysis. These documents need to be sorted and identified with a key number and an emphasis on making the information accessible.

All documents have common requirements, they must be:

- **Available when needed**: As in all human endeavours, time is a constraint in IT; documents must be available on request as most of the time the particular information sought will help decision-making.
- **Easy to find**: In order to retrieve a document (to find a piece of information or update it) efficiently, it must be stored under a classification scheme.
- **Current** (up-to-date): Normally, a document has an owner who is in charge of maintaining it, but in order to update a document, a business process called 'change control' must be followed.

Change control is the process of managing and controlling changes; requested or otherwise. It ensures that all work is justified and that all work requested and approved is completed and tested. In some organisations, no change can be made without an approved change control form.

2.5 Valuable originals and document security

Valuable original documents, possibly held in a protected place under the care of IT, may be:

- legal or historical papers
- signed forms
- Tender documents
- Contracts
- Agreements
- Warranties and licences.

These documents need to be sorted, identified with a key number, and filed (with a strong emphasis on security). They need to be accessible on a 'need to know basis' — this attribute is very important for information in IT documents that is confidential or sensitive and restricted to authorised access (specific individuals).

The objective of document security is to preserve the organisation's information assets and the business processes they support, by:

- **Confidentiality**: where documentation is accessible only to those authorised to have access
- **Integrity**: where accuracy and completeness of information contained in the documents and processing methods are safeguarded
- **Availability**: when documentation and associated assets are accessible by authorised users when required.
- Document and file properties

One simple way to protect a soft copy document is to use the built-in security file features, now common to operating systems. Using this system, every object has a unique owner who has control of and access to it. An object can be a folder, file (document) or a complete network drive. The access provided by the owner can be 'read', 'write' or 'no accesses. Owners can also revoke access to users. Typically, the department or a section within an organization appoints the owner. Normally, sensitive documentation is labeled 'commercial-in-confidence'.

Self Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. ----------Including manuals that come with hardware and software, needs to be stored correctly.
2. Which one the following is uses to access documentation only by authorized person. (2pts).
   A. Confidentiality:
   B. Availability
   C. Integrity:
3. ----------is use to check accuracy and completeness of information contained in the documents (2pts).
   A. Confidentiality:
   B. Availability
   C. Integrity:
4. What is difference between Confidentiality and availability (5pts)?
5. Explain berifley deffference b/n Documentation and Technical documents (5pts)

Note: Satisfactory rating - 3 and 5 points Unsatisfactory - below 3 and 5 points
You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Short Answer Questions

3.1 **Accessing stock and inventory**

3.1.1 Stock:- describes the goods that an organization currently holds. For example, if an organization makes computers, they need to keep a stock of hard disks, system boards, network cards, monitors, cabling and so on.

A person checking stock

3.1.2. Inventory: - is a list of what you actually have, and a description of it. For example, when you insure the contents of your house you are usually asked to perform an inventory of the contents, in order to calculate how much to insure it for.

Organisations need to keep track of how much stock they have — so that they don't run out of stock, as well as for insurance reasons. In addition, once a year all items may be counted manually to make sure that the computerised stock-control records correspond with what is actually on the shelves, a process known as **stock taking**.

3.2 Document control and distribution

In an IT organization or department, the controlled distribution of documentation is of paramount importance.

3.3 Levels of security and confidentiality

Security you should always store computer hardware and software in a secure place, in order to prevent theft. Access to a storeroom must be restricted to authorized personnel. Security also means protection against fire, flood, mould and insect pests.

You must also make sure that there are real connections between the stored stock and the inventory records. The inventory record of any document should show the security level.

3.3.1 High security — valuable originals

Some documents in the care of IT must be kept safe, perhaps in their original condition. They may hold trade secrets or confidential information. Some documents are held in a form that is liable to damage and must be kept in a secure area, not to be removed, with even authorised people only able to access copies or images of them.

3.3.2 High security — critical information and fragile media

Original documents that may have a critical value, or be recorded on a fragile medium such as tape, should not be allowed to leave their secure storage place. Only copies should be taken out.

3.3.3 Medium security — sensitive and restricted material

Some records contain sensitive material, and may not be seen by all employees. Each document and each authorised user of a system should be assigned a security level. Unauthorised people can be denied access to the whole system. If a person's security level were lower than the security level of a document or record, access would be denied.

3.3.4 Low security — general access required

Other documents might hold knowledge that is critical to the workings of IT equipment, but copies or images can be freely distributed, so long as the version of the document is clearly marked, and the reader has the necessary authority.

4. Hard copy documents

If a document is in hard copy, and the user is authorized to access it, the lender's details can be recorded in a simple database to keep track of it

5. Soft copy documents

Distribution can be made secure and tracked by granting access to only the appropriate documents (by pre-determined levels of security) and by sending documents by email and filing/registering a copy of the email.

If the customer is off site, the email attachment must be in a compatible format. In the case of intranet html documents, usage can be tracked by the number of times that the page has been accessed, and privileges can be allocated of access needs to be restricted.

6. Reporting, auditing and archiving documentation

Your manager could ask you for a report on who has been using the technical documents listed in the index or inventory. You may need to show what's been added, what's been deleted, or transferred.

You may be asked to extract from your index or inventory a summary of who has borrowed books, or taken, or even read various documents.

Technical records need regular auditing. You may be called on at intervals to check records and manuals. If so, you would look for items missing, damaged, misplaced, borrowed for too long, or materials that are out of date.

Some documents have to be kept, by law, for a certain amount of time and should be archived. Records or books that have not had any activity for a while can be transferred to archives, freeing up valuable space.

Self Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Security is protection against fire, flood, mould and insect pests.

A. True B. False

2. ---------- Is a list of what you actually have, and a description of it.

A. Inventory B. Stock D. Control E. All

3. ---------- Describes the goods that an organization currently holds.

A. Inventory B. Stock D. Control E. All

4. What is difference between Hard and Soft copy documents?

5. List down level of security?

1. -------
2. --------
3. --------
4. --------

Note: Satisfactory rating - 5 and 9 points Unsatisfactory - below 5 and 9 points
You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Short Answer for Question

Operation Sheet 1	**Accessing stock and inventory control** **Store securely technical documentation** **Store software, Hardware and Equipment not in use**

Techniques Access stock and inventory control

1. Level of inventory
2. Adjust Store room design, layout, location and security
3. Design considerations
4. Locating stores
5. Level of Security
6. Stock rotation

LAP TEST	Practical Demonstration

Name: _____ Date: _____

Time started: _____ Time finished: _____

Instructions: You are required to perform the following individually with the presence of your teacher.

Task 1. Apply Level of Inventory

Task 2. Check level of Security

Reference

1. **http://www.euro.who.int/data/assets/pdf_file/0007/115486/E77650.pdf**

2. **https://www.slideshare.net/catherinelvillanueva1/ict-83930037**
3. Samuel P. Harbison III & Guy L. Steele Jr, **C: A Reference Manual**, Fifth Edition,
4. Prentice Hall, 2002, http://www.CAReferenceManual.com,
5. Posted by Synopsys Editorial Team on Friday, October 7th, 2016

Experts

The development of this Learning Gide for the TVET Program Information technology support service Level I.

No	Name of Trainers	Phone Number	E-mail Address	Region
1	Abdulakim Ahemed	0921900418		Harari
2	Assefa Million	0911034866	amen192005@gmail.com	Harari
3	Derese Teshome	0913938439	dereseteshome@gmail.com	AA
4	Getenesh Osamo	0923816933	gete.osamo@gmail.com	SNNPR
5	Remedan Mohammed	0913478937	remedanm77@gmail.com	Harari
6	Sewayehu W/Yohanes	0911716733	Baroke0816@gmail.com	SNNPR
7	Damelash Yihalem	0911912015	demenati@gmail.com	Harari