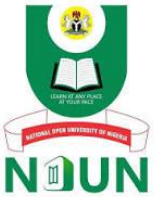
COURSE GUIDE

LIS 307
PRESERVATION AND SECURITY OF LIBRARY AND INFORMATION SYSTEMS AND RESOURCES

Course Team Nkata U. Kalu. PhD (Course Developer/Writer) - NOUN
Ukoha O. Igwe, PhD, CLN (Course Editor) – NOUN



NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
University Village
Plot 91, Cadastral Zone
Nnamdi Azikiwe Expressway
Jabi, Abuja

Lagos Office
14/16 Ahmadu Bello Way
Victoria Island, Lagos

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Printed 2022

ISBN: 978-978-058-240-1

Introduction

Welcome to **LIS 307:** Preservation and Security of Library and Information Systems and Resources. This is a two-credit (2-CR) unit course which is compulsory for all the undergraduate students in Library and Information Science department. The course is designed to enable you to explore and apply the principles and approaches of preservation and security of information systems and resources in the library. Also, it will empower you to achieve excellent personal and academic development.

Course Objectives

By the end of this course you will be able to:

- recognise the preservation and security of library and information systems and resources skills you require for a successful academic study and career.
- identify the techniques to develop effective skills required for preserving and securing library items.
- apply the strategies to become expert in preserving and securing library materials throughout your study and beyond.
- determine the methods and procedures for preserving and securing library and information systems and resources
- recognise the factors that causes deterioration of information resources in the library.
- identify the challenges of preservation and security of library and information systems and resources in Nigeria

Working through this Course

To successfully complete this course, you are required to participate in both the theoretical and practical parts of the course. You are also to read the study units, listen to the audios and videos, do all assessments, examine the links and read, participate in discussion forums; read the recommended books and other materials provided, prepare your portfolios, and participate in the online facilitation.

Each study unit has introduction, intended learning outcomes, the main content, summary conclusion, and references/further readings. The introduction opens the door to each unit and gives a glimpse of the expectations in the study unit. Read and note the intended learning outcomes (ILOs) which outlines what you should be able to do at the completion of each study unit. This will help you evaluate your learning at the end of each unit to ensure you have achieved the designed objectives (outcomes). To achieve the intended learning outcomes, the content of each section is presented in modules and units with videos and links to other sources to enhance your study. Click on the links as may be directed but where you are reading the text offline, you may have to copy

and paste the link address into a browser. You can download the audios and videos to view offline. You can also print or download the texts and save in your computer or external drive. The unit summaries provide a recapitulation of the essential points in the unit. It's an indispensable brief that garnishes your journey through the unit. The conclusion brings you to the climax of the study and what you should be taking away from the unit.

There are two main forms of assessments – the formative and the summative. The formative assessments will help you monitor your learning. This is presented as in-text questions, discussion forums and Self-Assessment Exercises. The summative assessments would be used by the university to evaluate your academic performance. This will be given as Computer-Based Test (CBT) which serves as continuous assessment and final examinations. A minimum of three computer-based tests will be given with only one final examination at the end of the semester. You are required to take all the computer base tests and the final examination.

Study Units

There are 20 study units in this course divided into four modules. The modules and units are presented as follows:

Module 1	**The Definition of the Concepts of Preservation, conservation and security of library materials**
Unit 1	The definition and Concept of preservation in library services
Unit 2	Conversation of library and information materials
Unit 3	The Concept of security of library materials and resources
Unit 4	The Rationale for preservation, conservation and security of library items
Unit 5	The Importance of preservation, conservation and security of library resources
Module 2	**Methods and procedures for preserving and securing library and information systems and resources**
Unit 1	Principles of preservation, conservation and security of library items
Unit 2:	Policies and standards for preservation, conservation and security of library items
Unit 3:	Methods and procedure of preservation and security of library materials

Unit 4 Factors contributing to vulnerability of library materials

Unit 5 Regeneration and reprography of library resources

Module 3 Information Security

Unit 1 The information security and library services

Unit 2 Cryptology and network security

Unit 3 Issues in information security

Unit 4 Software security and authentication protocols

Unit 5: Principles and network security for security of library items

Module 4 Operational and Organisational Security

Unit 1 Operational and organisational information security

Unit 2 Data integrity, provenance and digital signatures.

Unit 3 Security and authentication protocols

Unit 4 Management and risk assessment

Unit 5 Challenges of preservation and security of library and information systems and resources in Nigeria

Presentation Schedule

The presentation schedule gives you the important dates for the completion of your computer-based tests, participation in forum discussions and at facilitation. Remember, you are to submit all your assignments at the appropriate time. You should guide against delays and plagiarisms in your work. Plagiarism is a criminal offence in academics and liable to heavy penalty.

Assessment

There are two main forms of assessments in this course that will be scored: The Continuous Assessments and the final examination. The continuous assessment shall be in three-folds. **There will be two Computer Based Assessments. The computer-based assessments will be given in accordance to university academic calendar. The timing must be strictly adhered to**. The Computer Based Assessments shall be scored a maximum of 10% each, while your participation in discussion forums and your portfolio presentation shall be scored maximum of 10% if you meet 75% participation. Therefore, the maximum score for continuous assessment shall be 30% which shall form part of the final grade. The final examination for LIS 211 will be a maximum of two hours and it takes 70 percent of the total course grade. The examination will consist of 70multiple choice questions that reflect cognitive reasoning.

Note: You will earn 10% score if you meet a minimum of 75% participation in the course forum discussions and in your portfolios otherwise you will lose the 10% in your total score. You will be required to upload your portfolio using Google Doc. What are you expected to do in your portfolio? Your portfolio should be note or jottings you made on each study unit and activities. This will include the time you spent on each unit or activity.

How to get the Most from the Course

To get the most in this course, you need a functional personal laptop and access to the Internet. This will study and learning easy and the course materials accessible anywhere and anytime. Use the Intended Learning Outcomes (ILOs) to guide your self-study in the course. At the end of every unit, examine yourself with the ILOs and see if you have achieved the outcomes.

Carefully work through each unit and make your notes. Join the online real time facilitation as scheduled. Where you miss a schedule for online real time facilitation, go through the recorded facilitation session at your convenience. Each real time facilitation session will be video recorded and posted on the platform. In addition to the real time facilitation, watch the video and audio recorded summary in each unit. The video/audio summaries are directed to the salient points in each unit. You can access the audio and videos by clicking on the links in the text or through the course page.

Work through all self-assessment exercises. Finally, obey the rules in the class.

Facilitation

You will receive online facilitation. The facilitation is learner centred. The mode of facilitation shall be asynchronous and synchronous. For the asynchronous facilitation, your facilitator will:

- Present the theme for the week;
- Direct and summarise forum discussions;
- Coordinate activities in the platform;
- Score and grade activities when needed;
- Upload scores into the university recommended platform;
- Support and help you to learn. In this regard personal mails may be sent;
- Send videos, audio lectures and podcasts to you.

For the synchronous:

- There will be eight hours of online real time contacts in the course. This will be through video conferencing in the Learning

Management System. The eight hours shall be of one-hour contact for eight times.

- At the end of each one-hour video conferencing, the video will be uploaded for viewing at your pace.
- The facilitator will concentrate on main themes that you must know in the course.
- The facilitator is to present the online real time video facilitation timetable at the beginning of the course.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

Do not hesitate to contact your facilitator. Contact your facilitator if you:

- do not understand any part of the study units or the assignments.
- have difficulty with the self-assessment exercises.
- have any question or problem with an assignment or with your tutor's comments on an assignment.

Also, use the contact provided for technical support.

Read all the comments and notes of your facilitator especially on your assignments; participate in the forums and discussions. This gives you the opportunity to socialise with others in the programme. You can discuss any problem encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the discussion session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help the university to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

Contents

MODULE 1: THE DEFINITION OF THE CONCEPTS OF PRESERVATION, CONSERVATION AND SECURITY OF LIBRARY MATERIALS

This module introduces you to the definitions and explanation of preservation, conservation, and information security. Also, it discusses the rationale and the importance of preservation, conservation, and information security of library items.

Unit 1 The definition and Concept of preservation in library services

Unit 2 Conversation of library materials

Unit 3 The Concept of security of library materials and resources

Unit 4 The Rationale for preservation, conservation and security of library items

Unit 5 The Importance of preservation, conservation and security of library resources

UNIT 1: THE CONCEPT OF PRESERVATION IN LIBRARY

CONTENTS

1.0 INTRODUCTION

This unit will help you to have more insight on the preservation, conservation and information security in library operations. Libraries are indispensable institutions in human existence, and library items are expensive to acquire, organise and disseminate. Therefore, it imperative to devise means and techniques to security the resources from human and natural disasters. Preservation denotes the activities directed at preserving and extending the life of library resources. To preserve and extend the life

of library materials, libraries device techniques and methods which are testable, practical functional. Our discussion here focuses on these techniques and the implications of each.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. appropriately define and explain the meaning of preservation in library operations;
ii. determine the various techniques and strategies for preserving library materials;
iii. ascertain the strengths and weaknesses of each preservation technique.

3.0 MAIN CONTENT

3.1 The Concept of Preservation in Library Operations

What is preservation?

Our discussion in this unit will be more meaningful with the proper definition of term preservation. What exactly is preservation? It is the process of protecting the life of library materials to extend their life expectancy. It can also be described as the activities that help to prevent deterioration of library items. Preservation can also be looked as the proper care, handling and storage of library materials. In library service provision, preservation is the act of preventive measure or activities aimed at prolonging the life cycle of books, records, or other library materials. The process of preservation often varies, generally, it include the amongst others the act of monitoring the condition of materials, maintaining the humidity and temperature of library collections both in the library and the store, in addition to the provision of disaster management plans, digitalisation and increasing access to the materials.

Preservation is an aspect of library services that is vital for survival of library items without it, references to prior publications/materials would have been difficult if not impossible. Ordinarily, we acquire library resources for future use, though we may at some point in time weed some, but such resources are kept mainly for future references and further research; therefore there is need for preservation. Both print and digital library resources are important to the library and users. Therefore, the lifespan or longevity of these materials depends largely on the manner they are handled, maintained and preserved.

Maintaining an adequate temperature needed for preserving library materials:
Source: https://www.google.com/imgres?imgurl=https%3A%2F%

The basic objective of a library is to collect, organize, preserve, and provide access to knowledge and information. In fulfilling this objective, libraries preserve a valuable record of culture that can be passed down to succeeding generations. Libraries are an essential link in this communication between the past, present, and future. Whether the cultural record is contained in books or in electronic formats, libraries ensure that the record is preserved and made available for later use (Kademani, Kalyane & Kumar 2003).

According to Osunride and Adetula (2017), the library is a repository of knowledge and a social institution saddled with the responsibility of disseminating knowledge to the people without discrimination. Information collections are the priceless heritage of mankind as they preserve facts, ideas, thoughts, accomplishments and evidence of human development in multifarious areas, ages and directions. Preserving intellectual and cultural heritage becomes not only the academic commitment but also the moral responsibility of librarians, who are in charge since proper dissemination of library materials is only possible when the documents are in good and usable condition.

Preservation is the art of 'keeping safe', 'maintaining', 'retaining', and 'keeping alive'. Preservation, as it applies to library and archive collections, can be defined as 'all managerial, technical and financial considerations applied to retard deterioration and extend the useful life of (collection) materials to ensure their continued availability (British Library 2001). According to Abatayo, (2019), preservation is the maintenance of library resources which is done to prevent (organic bodies) decay or spoiling of library materials. It is an activity that keeps library materials in perfect or unaltered condition.

It is worth to note that there are libraries with rare collections which may be refered to as people's heritage. The heritage reflect the culture and deserve to be preserved. It is the responsibility of the library to safeguard, protect and preserve these heritage and culture which may be in the forms of manuscripts, printed books, documents, palm leaves etc. Furthermore, preservation of library materials is a task that every library personnel and others outside the library must pursue.

Sarasvathy (2019) maintains that preservation measures have to be endorsed, supported and encouraged from the most senior level to the most junior in the library. Those who are responsible for managing the library and maintaining the external and internal fabric of the building should work closely with those who are responsible for the preservation of the collections. Preservation in the library should flow in line with the social and political climate in which the organisation operates. The organisation's purpose, collecting policies, and available resources also matter in preserving the wealth of resources available in the library.

The 21st century has marked the era of information explosion and revolution which has caused the increase in the volume of information being created and disseminated. Information and knowledge are growing faster, in multidisciplinary and dimensional forms. The information explosion has given rise to other forms of knowledge spinning around computing and communication tools which forms the backbone of the information and communication technology (ICT). This development has given rise to the concept of digital preservation.

What is digital preservation?

According to the Yale University Library Digital Preservation Policy (1999), digital preservation connotes all the activities and processes involved in the physical and intellectual security and technological stabilization of digital resources over time to replicate accurate copies of those resources. Digital preservation may involve many strategic plans aimed at protecting and providing access to digital content to ensure accuracy, mitigation and reduce or reverse the effect of obsolescence and media hardware and software.

Modern libraries maintain collections that include not only printed materials such as, books, periodicals, newspapers, and magazines, but

also art reproductions, films, sound and video recordings, maps, photographs, microfiches, microfilms, CD-ROMs, computer software, online databases, and other media. In addition to maintaining collections within library buildings, modern libraries often feature telecommunications links that provide users with access to information at remote sites.

As a matter of fact, information explosion has brought a change from prints materials such as books, newspapers, journals etc, to electronic/computer formats. This consequently has also resulted to change in the method of preserving such materials. This scenario according to Sarasvathy (2019), has given rise to the new dimensions of knowledge that not only accelerates its growth but has also transformed the nature of its resources from the printed form to the electronic/digital form such as magnetic tapes, floppy disks, CD-ROM, etc. The internet era however, brought a rapid development and growth of online databases, List Serves, discussion groups, electronic journals, etc which has enriched the accessibility of information.

The development of digital libraries or virtual libraries have further promoted library activities and have taken them beyond the formal library buildings. To this end, the shift in information creation, collection, organisation, storage, and dissemination has called for the technology and digital base preservation methods, procedure and policy.

3.2 Basic preservation Elements

According to Northeast Document Conservation Centre (NDCC) (2015), some of the activities involved in preserving library materials include:

- **Environmental Control**—'providing a moderate and stable temperature and humidity level as well as controlling exposure to light and pollutants. This should be a priority for all institutions, although this kind of control is more pronounced for rare books, special collections, or archival materials than for general circulating collections.

- **Disaster Planning**—this is preventing and responding to damage from water, fire, or other emergency situations. This should also be a high priority in all institutions. The reasons are obvious for collections of enduring value, but even collections that are not meant to be retained over the long term represent a capital investment for an institution and as such must be protected from loss.

- **Security**—protecting collections from theft and/or vandalism. This type of protection is needed for both special and general collections, since loss and vandalism of general collections results in unnecessary replacement and expense.

- **Storage and Handling**—using non-damaging storage enclosures and proper storage furniture; cleaning storage areas; using care when handling, exhibiting, or reformatting collections and educating staff and users in proper handling techniques. Storage and handling is imperative for all types of collections.

- **Reformatting**—reproducing deteriorating collections onto stable media to preserve the informational content or in cases where the originals are fragile or valuable and handling is restricted. This category includes microfilming, production of preservation facsimiles, and duplication of audio-visual collections. These strategies are most appropriate for collections whose intellectual content should be preserved over the long term and/or where security copies are needed for unique items. Microfilming is still an effective strategy for unique paper-based collections, but a low priority for institutions with general collections that are duplicated elsewhere.

- **Library Binding**—rebinding of damaged volumes to provide sturdy use copies. This strategy is used by libraries with general collections in heavy use. It should not be used on any items that have art factual value.

- **Conservation Treatment**—treating individual objects using the services of a trained conservator. This may be appropriate for a wide range of institutions which hold unique materials that are of sufficient value to justify treatment.

- **In-House Repair**—repairing objects that do not have artefactual value using a trained collections conservator or trained in-house staff. In-house book repair is used by public and academic libraries to keep non-unique books in good condition for use, and some institutions use basic paper repair techniques (e.g., mending, encapsulation) for historical materials. For special collections libraries, archives, and historical societies, general preventive activities such as rehousing should be given a higher priority than in-house repair.

- **Digital Reformatting and Preservation**—using digital imaging to provide access copies of deteriorated original collections; creating digital objects that will act as preservation copies of

original items; and/or preserving objects that are "born-digital." Digital projects may be appropriate across a wide range of institutions; the key in undertaking such a project is for the institution to have a good understanding of the requirements and limitations of digital imaging.'

4.0 CONCLUSION

Preservation of library and information materials has been a problem that affected the smooth running of library services. However, the advancement of information and communication technology has brought about the proliferation of information which appear to be overwhelming librarians and other information managers. This confers responsibility on libraries and librarians to ensure information resources and other materials in the library are well organised and preserved for longevity, easy access and use.

5.0 SUMMARY

This unit examined the definitions and meaning of preservation of library materials. Preservation was described as the process of 'keeping safe', 'maintaining', 'retaining', and 'keeping alive'. Librarians need to know that preservation is an aspect and or activity of library services that is vital for survival of library items, this is because the lifespan or longevity of these materials depends largely on the manner they are handled, maintained and preserved. We also explore some of the basic preservation elements which include environmental control, disaster planning, security, storage and handling as well as reformatting of library materials.

.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. Mention and explain the five elements of preservation discussed in this unit

These your tutor-marked assignment sounds too elementary

7.0 REFERENCES AND FURTHER READING

Abatayo, J. V. C. (2019). Preservation and conservation of library materials Retrieved from https://www.slideshare.net/JoloVanClydeAbatayo/preservation and conservation of library-materials-131548988. (27th October 2021)

Adekanni, J. O. & Wahab, W.W. (2015) Comparative analysis of the preservation and conservation techniques of selected special and

academic libraries in Retrieved from http://digitalcommons.unl.edu/libphilprac/1328 (6th March 2021).

British Library (2001) Basic preservation for library and archive collections https://www.bl.uk

IFLA (2010) Principles for the care and handling of library materials international preservation issues, Retrieved from http://archive.ifla.org/VI/news/pchlm.pdf. (8th March 2021).

Jordan K. S. (2003). *Special collections and preservation: In Encyclopedia of library and information science*. Chicago, Illinois USA: Chicago Public Library.

Kademani, B. S., Kalyane, V. L., Kuma, V. (2003) Preservation of information resources in libraries: new challenges-www.eprints.rclis.org

Northeast Document Conservation Centre (NDCC) (2015) Introduction to preservation. Retrieved from https://www.nedcc.org/preservation101/session-1 (28th October 2021).

Osunride, A. A. & Adetula, B.O.G. (2017) Preservation and conservation of library materials in university libraries in south-west, Nigeria. *International Journal of Library and Information Science Studies* Vol.3, No.3, pp.8-19

Popoola, S. O. (2003*). Preservation and conservation of information resources.* Ibadan: Distance Learning Centre

SANS (2006) Information security. Retrieved from https://www.sans.org/information-security/ (4th April 2021)

Sarasvathy, P. (2019). Preservation and conservation of rare materials in select libraries in Karnataka a study. Retrieved From: http://hdl.handle.net/10603/73608 (28th October. 2021)

Yale University Library's digital preservation policy framework (1999) https://web.library.yale.edu/sites

UNIT 2: CONSERVATION OF LIBRARY MATERIALS

CONTENTS

1.0 INTRODUCTION

Recall that we discussed preservation as activities aimed at extending the lifespan of library items. Conservation refers to the physical treatment of mutilated or damaged library materials. Libraries and information centres are often confronted with care and handling of materials that require physical measures to rebuild, bind or repair mutilated library items. This is the focus of conservation. What are the various methods that libraries deploy to care for damaged items? This is the central discussion of this unit.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to

i. define and explain the meaning of conservation in library services;
ii. identify the various techniques in the conservation processes;
iii. discuss the threats to the library and information materials

3.0 MAIN CONTENT

3.1 Conservation:

The act of conservation of library materials is a major responsibility of librarians and libraries in the efforts to provide good and quality service delivery to the clients.

The process of conserving library materials for longevity: Source: lisbdnetwork.com

What is Conservation?

What do you understand by the term conservation? Ordinarily conservation and preservation have been mistaken to mean the same thing. Interestingly, some literature/scholars often use the two terms interchangeably. Do they really mean the same thing? A closer examination of their definitions, tasks involved and the applicability of the two concepts illustrate a clear difference. According to IFLA (2010), preservation and conservation are two words that have relatively different implications though they are related to each other and can be used interchangeably in extreme cases. Generally, preservation can be defined as deliberately calculated activities in sustaining library and archival materials either in their original or other readable format for further references, while conservation is part of preservation processes/activities that employs preventive measures to repair damaged materials for further usage. The IFLA Principles for the Care and Handling of Library materials (2010) also defines conservation as specific practices taken to slow down deterioration and prolong the lifespan of an object by direct intervening in its physical or chemical make-up.

Akambi and Wahab (2015) maintain that Conservation is part of the processes of keeping an object safe from harm or loss, damage, destruction and maintaining it in a reasonably sound condition for present and future use. While preservation deals with the regular maintenance aspect, conservation deals with the curative treatment. Alegbeleye (2002) states that there are few misconceptions in the use of preservation and conservation. He explains that the terms are used interchangeably even

though strictly speaking, experts in the field draw a distinction between the two words.

Preservation includes all the managerial and financial considerations, including storage and accommodation provisions, staffing levels, policies, techniques and methods involved in preserving library and archival materials and information contained in them. Conservation on the other hand, refers to specific practices taken to slow deterioration and prolong the life of an object by directly intervening in its physical or chemical make-up.

Usually, library materials are frequently used by the clients and this process expose the materials and make them vulnerable to wane, tear and damage. Based on this, a process is therefore needed to restore or bring back to life such materials that are in the process of being destroyed. This is where conservation sets in. This treatment of physically damaged library resources to extend their usage captures the essence of conservation processes.

Conservation practices are focused at ensuring that significant library and archive materials, published and unpublished, in all formats are kept in accessible form for as long as possible. It is the practice of minimizing or reducing the physical and chemical deterioration of documents.

Jordan (2003) describes conservation as an umbrella term for an array of activities, principles, practices, and organisations that ensure the usability, longevity, and accessibility of recorded knowledge. These activities include general collections repair, reformatting (microfilming, photocopying, and digitization), environmental monitoring and control, care and handling of materials, disaster preparedness and recovery, binding and preservation education and training.

Generally, conservation activities in the library include:

- repair of library items
- restoration of library materials from loss, damage or neglect
- treatment of physically damaged materials to extend their life
- examination (regularly) of the library materials,
- documentation and
- preventive care (Northeast Document Conservation Centre (NDCC), 2015)

3.2 Techniques of Conservation

There are two main practices that are involved in salvaging the deteriorating materials in the library, which include the following:

- **Preventive Conservation***:* This involves the defensive aspect of protecting materials for continuity. Furthermore, it is an act of taking sufficient measures to control or manipulate environmental

factors such as temperature, humidity, ultraviolet radiance which act as a check to deteriorating agents.

- **Interventive Conservation***:* This aspect of conservation involves the direct dealings involving the conservator and the material to be preserved. Activities here include; repairs, cleaning, consolidation, stabilizing and/or complete replacement

3.3 Threat to Library and Information Materials

Several activities pose as threats to the library and information materials world over. One of such enemies of information materials is the librarian who fails in his duty to preserve the information materials under his care. However, preservation in the digital world is not absolute, but depends instead on the continuing transformative impact of the digital product on the information work of end-users. Other threats arise from the following:

- **The way the information material is handled:** Storage and handling methods have a direct impact on the useful life of collections and the accessibility of information. Damage to collections can be avoided by preventing overcrowded, careless, or haphazard storage conditions
- **The nature of the material itself**: While various materials and formats have special preservation needs, there are a few recommendations that are common to the long-term preservation of nearly every type of item. These recommendations deal with temperature, relative humidity, light, and air quality.
- **Natural and man-made disasters**: Disaster occurrence are often common among human beings. While some are beyond man's control, others occur due man's negligence of uncoordinated activities. Those that occur as a result of natural activities are natural disasters and include floods, fires, volcanoes earthquake, tornadoes etc. whereas, man-made disasters include war, hazardous exposure, pollution, nuclear explosions, accidents etc.
- **The way the material is handled:** There is the need to make a comprehensive and honest assessment of the physical state of collections and their preservation techniques by any library or information centre in order to be able to care for its collections. Both the user and the librarian each has a big role to play in the way materials are handled. A careful handling of materials will result to its longevity and vice versa. Therefore, experts in conservation are trained to affect conservation treatment techniques and provide recommendations for long-term preservation of information materials in suitable environments.
- **The environment in which it is kept:** The nature of the surrounding, atmospheric condition and the general setting of where information materials are kept/preserved would have

negative or positive effect on its preservation. Accordingly, high temperatures, high humidity, or large fluctuations or changes in temperature and humidity can damage most materials. High humidity encourages the growth of mole and mildew and affects the chemical makeup of items such as film, photographic prints, and audiotape or videotape

4.0 CONCLUSION

The way and manner to conserve library and information materials have been an issue from the inception of librarianship. This has also affected the library operations due to inability to conserve and maintain some delicate and valued materials. Conservation is to ensure that significant library and archive materials, published and unpublished, in all formats are conserved in accessible form for as long as possible. Hence, the practice enhances minimizing or reducing the physical and chemical deterioration of library materials.

5.0 SUMMARY

We have learnt in this unit, the definitions and meaning of conservation of library materials. You have been exposed also to the techniques of conservation, threats to library materials as well as conservation activities which include to repair, treat, examination, restoration and preventive care among others.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. Discuss the various practical steps libraries employ to protect expensive and rare resources

7.0 REFERENCES AND FURTHER READING

Akambi, J. O. & Wahab, W.W. (2015) Comparative analysis of the preservation and conservation techniques of selected special and academic libraries in Retrieved from http://digitalcommons.unl.edu/libphilprac/1328 (6th March 2021)

Alegbeleye, G.O. (2007) *Media deterioration: the case of microfilm damage at the National Archives of Nigeria and the University of Ibadan*. University press. Ibadan

Northeast Document Conservation Centre (NDCC) (2015) Introduction to preservation. Retrieved from https://www.nedcc.org/preservation101/session-1 (28th October 2021)

Osunride, A. A. & Adetula, B.O.G. (2017) Preservation and conservation of library materials in university libraries in south-west, Nigeria. *International Journal of Library and Information Science Studies* Vol.3, No.3, pp.8-19

Popoola, S. O. (2003*). Preservation and conservation of information resources.* Ibadan: Distance Learning Centre

UNIT 3: THE CONCEPT OF INFORMATION SECURITY (*INFOSEC)* IN LIBRARY

CONTENTS

1.0 INTRODUCTION

Information security, also referred to as infosec is a major concern to libraries and information centres. Building and developing an information centre involves a lot financial responsibility. Gathering and organizing information resources is tasking and laborious. Therefore, libraries and librarians pay attention to secure their resources and minimize or mitigate information risks. There are several strategies or measures that libraries deploy to mitigate information risks. Different libraries handle the subject of information security in ways that are peculiar to their environment and the nature of the clients. The environment of academic libraries is substantially different from public or research libraries; so is the issue of information security. This unit brings *infosec* to focus on information circles particularly libraries.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. explain the meaning of information security in library services
ii. analyse the principles and applicability of information security to library operations
iii. identify the practical steps libraries adopt to secure their items

3.0 MAIN CONTENT

The word ‘security’ is derived from the Latin word ‘*secures*’ which literally means ‘free from danger’. In other word, the state of being secured. According to Fischer and Green (1998), security implies a stable,

relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury.

3.1 Information security in library operations

Concept of Information Security '*Infosec*'

What is Information Security?

Generally, security involves safeguarding and prevention for safety. It can also be seen as freedom from attack and potential harm from others. Information security has therefore become the process or measure of protecting against an unauthorised access and use of information or data weather in print or electronic format. There are many definitions of information security '*infosec*. In essence, different scholars define it according to their discipline and schools of thought.

Information security. Source: https://encrypted-tbn0.gstatic.com

According to Fruhlinger (2020), information security is a set of practices intended to keep data secured from unauthorised access or alteration, both when it is being stored and when it's being transmitted from one machine or physical location to another. Information security might as well be referred to as data security. It is obvious that knowledge has become one of the 21st century important assets. Therefore, efforts to keep them secured have correspondingly become increasing important.

SANS (2006) maintains that information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

According to CSRC (2019), the term 'information security' means protecting information and information systems from unauthorized

access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability.

Information security: Source: www.*intigrow.com*

3.5 Principles of Information Security

An institution that uses computers and other information bearing electronic devices ought to know and describe their information security needs as well as trust the system in which the security of the information will be built on. To secure a formidable information security, players and owners of the information as a matter of fact must adhere to the basic principles it requires. The three major principles/requirements of information security process include:

A. ***Confidentiality:*** This has to do with maintaining the privacy and secrecy of information or data and having firm control of its access and use.

B. ***Integrity:*** This type of requirement deals with the ability to ensure that information and program do not change without the authority of the institution or individual that owns it, hence, change can only come in a specific and approved manner.

C. ***Availability:*** The principle of availability ensures that only authorised users get continued access to the available information and resource in the system.

Information principle: Source: www.intigrow.com

4.0 CONCLUSION

The security of information resources have been a problem that has affected the smooth running of library services. It is obvious that the advancement of Information and Communication Technology has brought the proliferation of information which seems to overwhelm librarians and other information managers. However, it remains the responsibility of the libraries and librarians to ensure information resources and other materials in the library are well organised and secured for safety, longevity, access control and use.

5.0 SUMMARY

This unit examined the definitions and meaning of information security. Information security was describe as a set of practices intended to keep data secured from unauthorised access or alteration (both printed and digital). We also discussed the principles of information security which include confidentiality, integrity and availability. These principles serve as the code through which information security is built on.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. Mention and explain the three characteristics on which the principles of information security are built?

7.0 REFERENCES AND FURTHER READING

Computer Security Resource Center (CSRC) (2019) *Cybersecurity Supply Chain Risk Management.* Accessed from**:** https://csrc.nist.rip/ (4th January 2021).

Fischer, R. J. & Green, G. (1998). Introduction to security. Accessed from: https://books.google.com.ng/books/about/Introduction_to_Security.html?id=8 mmYBsBFrDgC&rediresc=y (3rd June 2021)

Fruhlinger, J. (2020) Information security and practices Retrieved from https://www.sans.org/information-security (6th March 2021)

SANS (2006) Information security. Retrieved from https://www.sans.org/information-security/ (4th April 2021)

UNIT 4: RATIONALE FOR PRESERVATION, CONSERVATION AND SECURITY OF LIBRARY ITEMS

CONTENTS

1.0 INTRODUCTION

In this unit, we will explore the rationale for the preservation, conservation and security of library materials. This will provide the bedrock for the practices of libraries on preservation, conservation and security of library items. It is important to bring to the fore the reasons and the motivating factors behind preserving and conserving library items as well as why the security of library items is important.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. analyse the rationale for the preservation of library materials;
ii. explain the need for the security of library items
iii. identify reasons for conservation of library materials.

3.0 MAIN CONTENT

According to Aina, (2003) preservation is the maintenance of library and information materials so that they can remain closely in their original condition as much as possible. It is mandatory that librarians ought to know the need for this practice and adhere to it in order to provide effective service delivery.

3.1 Rationale for the preservation of library materials

The Encyclopaedia of Communication and Information (2021) states that preservation involves maintaining an object or information in a format that the continued use and accessibility is guaranteed. It also involves the preparation of library items against the potentials of disaster such fire, earthquake, flood, hurricane, tornadoes etc. The following are the rationale for preservation of library materials thus:

1. **For future use and reference**: Every library material is regarded as a prospect, therefore preservation is needed for further utilisation, access, consultations as well as reference.
2. **To slow down deteriorating rate:** The rate of fading or weakening of library materials is reduced when proper preservative measures are taken.
3. **To reduce the risk of damage:** The draft and implementation of preservation policy ensures a sure way to guard against unforeseen occurrences in the form of disaster that may destroy library materials.
4. **To retain compendium of information:** Materials and information resources in the library such as political, economic, social and findings/discoveries from scientific research are life threatening issues when lost or damaged, therefore preservation of such materials is extremely important.
5. **To preserve the raw materials of history:** Library materials provide background information concerning events and occurrences in history that are vital for generational use and references. Therefore, preservation should be done for this reason.
6. **To protect materials to cater for a wide range of users:** Preservation practices such as photocopying, and digitalisation make it possible to have many copies available in different formats especially the hard copies.

3.2 Rationale for the conservation of library materials

Conservation is considered as a specialised practice of making fragile library materials safe and/or extending the usability and lifespan of such items. It involves the application of various strategies used for safeguarding the items from deteriorating or decay. Libraries and librarians usually employ several techniques and strategies to ensure these materials are well taken care of and safeguarded.

Librarian/Conservator activities includes:

1. Duplication: It is a practice whereby heavily/constantly used materials are identified and doubled via duplicating. This process includes scanning, photocopying, microfilming etc.

2. Physical treatment of library materials: This implies the ability to restore the damaged or deteriorating materials to expand its life span and usage.
3. Migration to digital: Moving from the traditional librarianship to digital or e-library by creating a negative format of the original in order to preserve them. In other words, migrating original materials into a recent technology.

Why should we conserve library materials?

The need for conservation of library materials cannot be overemphasized. According to Palmer (nd) the following are the reasons for library materials conservation:

1. Conservation helps in preserving useful and valued library materials
2. It is cost effective compared to outright purchase of new collections.
3. It enhances the preservation of unique and original materials in the library's special collection, especially the cultural heritage.
4. Conservation assists the library conserve fund for the purchase of new and additional materials through cutting replacement cost of the old materials
5. Conservation promotes cultural diffusion by allowing each items of the cultural heritage to be in circulation as long as it is needed.
6. It provides the library users the opportunity to have access to varieties of materials especially the old ones.
7. Conservation is useful, for the fact that it creates opportunity to protect current and future library collections.
8. Without conservation, the materials that are not online would deteriorate, decay and damage.
9. Conserving library collections protects and chronicles the past, communicates present and helps shape the future.
10. It helps in keeping people informed as well as proving a levelling field for access to resources.

3.3 Rationale for information security in the library

The two main threats to library materials are man-made and natural disaster. Therefore, it is good to employ proper measures in protecting these materials from loss, mutilation or total damage. Both threats and disasters pose great danger to the library items. For the fact that we cannot stop the natural disaster from happening, the least we could do is, prepare to face it properly with lesser damage (Dawar, 2016).

Reasons for security of library items

In every library, the resources and materials are highly prized, valued and constitute their very existence. Generally, these items are exposed to all manner of threats and danger. Therefore, without any deliberate steps to secure them, the entire library resources are vulnerable to unwanted access, mishandling, pilfering and even to intruders. Some of the reasons for information security or *inforsec* can be highlighted as thus:

1. Effective information security measures facilitate stability and confidence.
2. To protection library materials in computerisation
3. Reduces threat of damage, theft, subversion, or sabotage.
4. Safeguards valued information from modification, disclosure, damage and unauthorised access
5. Protects users' personal information from hackers, misuse and theft.
6. Safeguards critical information such as: research data, personal information of scientists, staff and students, and sensitive information from criminals and terrorists.
7. Unsecured information causes leakages which can lead to loss of grants.

4.0 CONCLUSION

The rationale for the preservation, conservation and security of library materials forms key aspects of service delivery in the library. The processes are to ensure longevity of the library materials and enhance the control and safety of the resources.

5.0 SUMMARY

In summary, preservation, conservation and security of library materials are indispensable in library services delivery. This is important because preservation involves securing the items for future use and reference, while conservation helps in protecting current and future library collections; provides the library users the opportunity to have access to varieties of materials especially the old ones. Similarly, security of information resources ensures effective measures that facilitates stability, confidence and the protection of library materials in computerisation

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. The dynamics of information and the permeation of information and communications technology continues to transform the field of librarianship. In the light of the myriads of developments, discuss the necessity of preservation in library operations in the 21st century.

2. As a contemporary modern librarian, why do you consider it necessary to provide adequate security for library resources and materials?

7.0 REFERENCES AND FURTHER READING

Aina, L. O. (2003). Library and information science text for Africa. Accessed from:
https://www.researchgate.net/publication/269788918

Dawar, V. (2016) Digital information security for academic libraries. A paper presented at the Future Librarianship: Innovation for excellence. April 2016. Retrieved from https://www.researchgate.net/publication/335389774 (8th November 2021)

Encyclopaedia of Communication and Information (2021). Accessed from:

https://www.amazon.com/Encyclopedia-Communication-Information-3-Set/dp/0028653866

UNIT 5: IMPORTANCE OF PRESERVATION, CONSERVATION AND SECUIRYT OF LIBRARY RESOURCES

CONTENTS

1.0 INTRODUCTION

As earlier discussed, preservation, conservation and security of library materials are indispensable component of every library operation across geographical boundaries and in all ages. Libraries take deliberate steps to secure and prevent their resources to unauthorised access and mitigate them against man-made and natural disasters. Libraries will go into extinction if their collections are carelessly exposed to threats, dangers and disasters. It is imperative therefore, to examine the importance of all the techniques libraries and information centres deploy to preserve, conserve and security their resources.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to

i. explain the significance of preservation of library materials;
ii. identify the need for the security of library items
iii. recognise the significance of conservation of library items.

3.0 MAIN CONTENT

Information security implies a stable, relatively predicable situation in which information resources are saved without disruption, unwanted access or from damage. In other words, information security in the library involves protecting and safeguarding both the prints and non-prints of

library collections. Print and non-print in library collections pose peculiar precautionary measures to protect them. The print materials comparatively are simpler to protect while the non-prints which include the digital and the analogue are formats that require different forms of protection. Effective library security policies provide the environment to prevent harm or loss of information.

Threat to library materials

Specifically, a threat to library materials in any type of library, is any circumstance, person(s), events that threaten the safety and security of library materials. The level of vulnerability of the library material often corresponds with the degree of threat realizable on it. For instance, Dawar (2016) maintains that in system and network security, threats remain present but are mitigated through the proper use of security features and procedures. Mitigation is any effort to prevent the threat from having a negative impact, or to limit the damage where total prevention is not possible, or to improve the speed or effectiveness of the recovery efforts.

3.1 Importance of security of library materials

One of the major tasks in library service provision is to protect library resources (both print and non-prints) to avoid damage, theft, alteration, diversion or attack of any nature. Hence, the security of library materials revolves around the security policy, access control mechanism, breach detection structures, and anti-virus plans which are part of the examples that are applied in protecting the information from potential danger, threats or risks. The importance of information security to the information owner and users are highlighted as follows:

1. It guards the materials from pilfering, mutilation or damage and ensures maximum effectiveness and usefulness of items
2. It provides a relative measure security and safeguards the technology used in the library
3. It enables safe operational systems
4. It protects and safeguards the data collected either by the library or individual persons

3.2 Importance of preservation of library materials

There are multiple gains to derive in preserving library materials which include:

1. Prolonging the existence of library materials
2. Protection library materials through activities that minimise physical and chemical damage, decay and deterioration
3. Preservation helps in preventing bacterial growth in the materials
4. It provides the users the opportunity to have access to some valuable information of cultural heritage.

5. Helps in extending the life span of library items

3.3 Importance of conservation of library materials

Library materials are vital assets to knowledge and information seekers. Therefore, conserving them is important as indicated below:

1. It helps in keeping library resources for as long as possible
2. It gives the opportunity for longer use and access
3. It reduces recycling process thereby reducing the pressure on the earth's ecosystem
4. Well conserved library materials give clients the opportunity to have variety of information resources.

4.0 CONCLUSION

The importance of preservation, conservation and information security in the library cannot be overemphasised. Therefore, it is the duty of every librarian and information manager to adopt or adapt whichever method, tools and mechanism through which library materials could be preserved, conserved and secured for posterity.

5.0 SUMMARY

In this unit, we have discussed the importance of preservation, conservation and information security in the library. Conservation is important because it provides support in keeping library resources for as long as possible and gives the opportunity for longer use and access. On the other hand, information security is important because it provides the ability to perform effectively and safeguard the technology used in the library. Similarly, preservation helps in prolonging the existence and protection of library materials through activities that minimise physical and chemical damage, decay and deterioration.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

What benefits would the National Open University Library derive from preserving their library materials?

7.0 REFERENCES AND FURTHER READING

Dawar, V. (2016) Digital information security for academic libraries. A paper presented at the Future Librarianship: Innovation for excellence. April 2016. Retrieved from https://www.researchgate.net/publication/335389774 (8th November 2021)

MODULE 2: METHODS AND PROCEDURES FOR PRESERVING AND SECURING LIBRARY AND INFORMATION SYSTEMS AND RESOURCES

Unit 1 Principles of preservation, conservation and security of library items

Unit 2: Policies and standards for preservation, conservation and security of library items

Unit 3: Methods and procedures of preservation and security of library materials

Unit 4 Factors contributing to vulnerability of library materials

Unit 5 Regeneration and Reprography of library resources

UNIT 1 PRINCIPLES OF PRESERVATION, CONSERVATION AND SECURITY OF LIBRARY ITEMS

CONTENTS

1.0 INTRODUCTION

This unit introduces you to the journey of libraries in preservation and some of the intricacies in ensuring operational efficiency. Our discussion will bring to limelight some of the techniques libraries adopt to ensure their materials are safe, secure and preserved.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

At the end of your study in this unit, you should be able to:

i. identify the basic principles of preservation,
ii. determine the various factors necessary before preservation and conservation decisions are taken and
iii. apply the identified factors to any library of your choice

3.0 MAIN CONTENT

The principles of preservation and conservation of library resources by the librarians is aimed at establishing a responsible attitude to actualise preservation and conservation. It also serves as a statement that embodies a general approach to the nature and aim of preserving and conserving the related library materials work, however, the principles do not provide a broad list of detailed techniques and practices, hence it is the task aimed at minimizing or reducing the physical and chemical deterioration of library materials.

Book preservation and conservation. Source https://www.google.com/imgres?imgurl

3.1 Basics of preservation principles

Library preservation and conservation policies are made and updated according to the principles adopted by experts in the field and professional

librarians. This is to create standards through which library materials can be retained and maintained. There are seven basic principles in preservation and conservation of library materials which are itemised below:

1. **Maintaining the essential character:** Librarians and indeed all libraries should be conversant with the act of maintaining resources and recognise that the items are as important as acquiring them and maintaining them is part of essential responsibilities of librarianship. Therefore, they should maintain such operation principles that would compel returning materials to their location in the same condition they were received; keeping pets from the library materials; keeping foods and drinks away from the library and avoiding materials from getting wet, etc
2. **Prevention of deterioration:** This is a practice of preventing or keeping materials from deterioration before preservative and conservative measures are applied**.** Constant checks or examining of library items is indispensable to ensure molds, termites, dew, heat etc do not infest and degrade the materials before efforts are taken to treat them.
3. **Restoration:** This is the practice of refurbishing the library materials that are either damaged or losing its original form
4. **Rehabilitation:** This principle indicates that the library materials that are repaired should be reintegrated with other materials for users to have access to them
5. **Reproduction:** This is a process of duplicating library materials to avoid total loss when it is damaged. This could take the form photocopying
6. **Reconstruction:** This is a practice where some old and vital materials are reformed and modernised for present use

3.2 Factors to be determined before Preservation and Conversation decision

Preservation and conservation decisions are dependent on a variety of factors**,** and these include:

- The value of the information or intellectual content an object provides.
- The uniqueness or rarity of an object;
- Its connection with significant events, individuals, or places;
- Its significance in relation to an institution and the mission of that institution;
- Whether the information provided by the object is available elsewhere; and

- The consequences of the loss of the item or the information it contains.
- The current condition of an object, including its fragility and level of deterioration or wear that has occurred during its use serves as an important factor in preservation and conservation

Libraries have always struggled against the destruction of their resource from disaster agents such as fires, floods, earthquakes and wars. These destructive agents have affected countless libraries and their resources. Disasters have put an end to much of the recorded history of human civilization. Moreover, library materials also fall victim to slow decay caused by acid content on paper, insect infestation, improper storage or handling, and excessive heat, mildew, humidity, and air pollution. It is worth to note that environmental conditions and methods of storage have a great influence on the preservation of documents. All these identified agents when unattended to eat up the resources of libraries or lead to slow decomposition of essential resources. The slow decomposition of library materials is a universal problem. To ensure that library materials remain available to present and future generations of library users, libraries must therefore engage in a variety of preservation efforts.

These preservative efforts include the conservation of original materials and the transfer of information from original materials to more durable formats. Preservation does not simply happen on its own. A well thought out plan must be drawn and managed. Accordingly, the fifth Law of Library Science states that 'Library is a growing organism.' Which translates that libraries acquire information resource of all kinds unceasingly, and promote the use of these acquired materials. These resources are likely to damage as more users gain legitimate access and utilise them. Hence, to prevent the deterioration of such materials which may affect the retrieval of the contents, librarians need to adopt an array of appropriate management strategies. Beside other strategies, the control of the environmental conditions and the provision of good storage conditions constitute some of the best preventive measures.

4.0 CONCLUSION

The principles of preservation and conversation of information material forms a major task in librarianship without which library materials will continuously suffer great lose/damage. Hence it is the responsibility of librarians to apply the necessary principles in order to keep both the chemical and physical components of the library materials in usable forms.

5.0 SUMMARY

In this unit, we have discussed the principles that guide librarians in preserving and conserving library materials. The principle of preservation and conservation is the task that is aimed at minimizing or reducing the physical and chemical deterioration of library materials. Seven principles were listed and discussed thus:

- Maintaining the essential character
- Prevention of deterioration
- Consolidation of the fabrics
- Restoration
- Rehabilitation
- Reproduction
- Reconstruction

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. Preservation and conservation are indispensable in the operations of libraries today. Discuss their operational principles in the effective handling of library materials
2. Libraries and information centres are prone to insect infestation, improper storage or handling, and excessive heat, mildew, humidity, and air pollution. What measures can guarantee safety and security of library items from these destructive agents?

7.0 REFERENCES AND FURTHER READING

France, F. G. (nd) Best practice and standards in environmental preservation for cultural heritage institutions: goals, knowledge, gaps. Retrieved from

University of North Georgia (2013) Library consolidation to bring many benefits. Retrieved from https://ung.edu/news/articles/2013/08 (9th January 2021)

https://www.loc.gov/preservation/resources/staffpubs/France%20Best%20Pract ices. (2nd February 2021)

UNIT 2 POLICIES AND STANDARDS OF PRESERVATION, CONSERVATION AND SECURITY OF LIBRARY ITEMS

CONTENTS

1.0 INTRODUCTION

Library collections are preserved to be accessed and utilized. The materials form the vital sources which must be preserved and conserved to prevent decay, loss and damage. This unit introduces you to library policies that guide preservation and conservation practices.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

At the end of this unit, you should be able to:

i. identify the various preservation and conservation policies in library operations
ii. recognise the benefits of preservation policies in libraries
iii. identify the checklists for preservation policies.

3.0 MAIN CONTENT

Library resources and collections are composed mainly of organic materials which are subject to natural weakening. Most often, many of the materials such as paper are composed of some chemical substances during the production process that reduce their lifespan. Hence, to safeguard and prolong the lifespan of these materials, certain standards should be in place. Akande (2010) asserted that there can be no serious commitment to preservation programme without a policy, which will guide efforts at solving identified preservation problems.

Also, Ngulube (2005) described preservation policies for information resources as indispensable tools for organisations that are committed to facilitating the survival of information materials in their custody. Policies, therefore, are very crucial to facilitate survival of information resources in libraries. Policies are important because they set out goals to be achieved as well as guidelines for implementing the goals. Policies also facilitate a creative allocation of funds, staff, and other specific aspects of implementation and monitoring of preservation standard.

Preservation policy is made to serve as a guide in maintaining and conserving the library materials from decay. A good preservation policy must take account of the following elements:

- the goal and objective of the library and the institution
- the collection development policies or principles adopted by the library and the institution
- the significance of the individual library material
- the operational design and strategic plans
- the place of the library within the institution and international framework
- the need of the users

3.1 Categories of Information Resources

There are three main categories of information resources that the preservation policy are to cover. These include:

- **Print Resources:** This forms the major resources in the original/traditional library. It includes the books, newspapers, magazine, journals, periodicals, maps, as well as reference and non-reference materials etc.
- **Non-print Resources:** These categories of resources are not usually produced on paper. The use and application of these resources depend on the sense of sight, hearing or the combination of both thus:
  Audio resources: This presents information via the sense of hearing. It includes audio recording tapes
  Visual resources: This form of resource present or convey information through the sense of sight such as charts, photographs, posters etc.
  Audio-Visual Resources: This conveys information through the combination of the sense of both sight and hearing such as television, home video, films which form the software, whereas the audio-visual hardware are the machineries or gadgets for using the software and these include video recorder, projector and record players.
- **Electronic Resources***:* These are the Information Communication Technology (ICT) based library resources which can only be accessed and used by computer literates. These include the

information resources in computer with internet connection, microcomputers with Compact Disk-Read-Only Memory (CD-ROM) etc.

The maintenance or preservation of library information materials either in print, non-print or electronic so that they can be closed to original condition as much as possible can be achieved through the formulation and adoption of a suitable preservation policy by the institutions and librarians.

3.2 Policies of Preservation and Conservation

It is often said that the decision to have a policy is one of the most difficult choices to make. Some argue that it is easier to avoid it, to run away from unforeseen criticisms. In other words, designing a policy is difficult. However, without a policy, the government, organisations, institutions and the library maybe floating aimlessly and without a planned direction or strategy.

What is a policy?

The Cambridge Dictionary (2010) defines policy as a set of ideas or a plan of what to do in a particular situation that has been agreed officially by a group, of people a business organisation etc. Also, Collins Dictionary (2009) defines policy as a set of ideas or plans that is used as a basis for making decision, especially in politics, economics or business. In essence, library preservation policy is a set of planned strategy or principles that guide actions, adopted by the library or institution towards the maintenance and protection of library materials.

Preservation is a part of the management of the library and its resources. The aim is to ensure that library information resources (prints, non-print, and electronics) survive in an easy to get and useable condition for as long as it is wanted. Preservation policy therefore serves as rules, procedures and or strategies through which library information resources/materials can be preserved for longevity, easy access, and usage. Though preservation policies may differ due to mission and vision of the institution and/or organisation, yet it serves the same purpose. In essence, preservation policies are built on the following structures.

- Administrative structure
- Planning
- Collection management
- Financial backing
- Environmental control
- Digital divide

Also, another element of preservation policy according to Foot (2013) include:

- A Selection for preservation: - based on priority setting according to objectives of the library, retention policy, significance/value/rarity of material, amount and kind of usage, physical condition
- Budgeting for preservation: resources needed; resources available
- Education and Training of all library staff, conservation and preservation staff, users
- Risk assessment and risk management
- Disaster control
- Policy for, or statement on, research and development
- Treatments: - Standards and benchmarks, types of material (e.g., paper vellum, bound, unbound, manuscript, print, newsprint, art on paper, scrolls, seals, etc.) - Non-print media (e.g., film, photograph, audio-visual material, electronic material, etc.)
- Statement of responsibility (including reviews, implementation and monitoring)

3.3 Checklist of Preservation Policy

When arranging a preservation policy, we should consider the planned audience and in what manner it will be used as well as what it includes. The checklist includes:

- Will the policy be available on the organisation's website?
- in reading rooms,
- as part of reader welcome pack and
- staff inductions

3.4 Benefits of Preservation and Conservation Policy

Foot (2013) listed the benefits of preservation policy to include among others to**:**

- clarify the relationship between the organisation's mission and preservation activity
- clarify the scope of preservation activity by identifying the collections to be preserved, their significance and the desired retention period.
- act as a focal point for collaborative working across organisations and in some cases between organisations
- clarify relationships with other aspects of collections management such as collections acquisition, access and security
- provide a statement of accountability against which performance can be monitored
- demonstrate the organisation's long-term commitment to its collections to funders and users, internal and external
- act as a communication tool, internally and externally

- provide a basis for the development of preservation strategy and preservation programmes
- provide a basis for establishing priorities and justifying investment
- demonstrate responsible stewardship for the benefit of current and future users
- explain to users why certain actions are taken and others are not

4.0 CONCLUSION

Preservation policy is the totality of plan embracing the overall goals and acceptable procedures aimed at maintaining and protecting the library materials from decay or deterioration.

5.0 SUMMARY

In this unit, we have discussed the preservation policy which is based on the structures such as administrative structure, planning, collection management, financial backing, environmental control and digital divide. Also, we have learnt the categories of information resources that are preserved in the library which include prints, non-prints and electronics material. In addition, the benefits and checklist of preservation policy were also discussed.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. Policies are guidelines to organisation's actions without which it would be difficult for the organisation to achieve its set goals. What would NOUN library stand to gain by formulating and applying library preservation and conservation policy?

7.0 REFERENCES AND FURTHER READING

Cambridge Dictionary (2010). What is policy? Retrieved from https://dictionary.cambridge.org/dictionary/english/policy (3rd March 2021)

Collins dictionary (2009) Policy. Retrieved from https://www.collins+dictionary&ie=utf8&oe=utf-8 **(**3rd March 2021)

Foot, M. M (2013) Building a preservation policy. Retrieved from https://www.bl.uk/britishlibrary/~/media/bl/global/conservation/pdf- guides/building-a-preservation-policy (4th April 2021)

Gertz, J. (2000). Selection for preservation in the digital Age: An overview. *Library Resources and technical services* .44.2: 97-104.

Retrieved from http://vweb.hwwilsonweb.com (7th March 2021)

International Federation of Library Association (2003). Audio-visual and multimedia section guidelines for audio-visual and multimedia materials in libraries draft June 2003. Retrieved from http://www.ifla.org/VII/s35/pubs/avmg103.htm. (22nd May 2019)

Menges, G. L. (2006). Preservation and conservation of library materials. Retrieved from http://www.lib.washinton.edu/preservation/preservationsyllabus2006.pdf. P.1418(2) (3rd March 2021)

National Library of Australia (2004) Preservation policy. Retrieved from http://www.nla.gov.au/policy/pres.html. (3rd March 2021)

Popoola, S. O. (2003). *Preservation and conservation of information resources*. Ibadan: Distance Learning Center, University of Ibadan, Ibadan. 3- 4.

UNIT 3 METHODS AND PROCEDURES OF PRESERVATION AND SECURITY OF LIBRARY MATERIALS

CONTENTS

1.0 INTRODUCTION

Preservation of library materials and systems is vital in the library service aimed at protecting and stabilising the library resources that are useful to the user. Therefore, librarians should have the knowledge of the way and manner library resources and systems should be preserved. The methods and procedures of preserving library materials is the focus of our discussion in this unit.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

This section brings you face to face with the methods and procedure of preservation and security of library materials. Hence, at the end of this unit, you are expected to/;

i. explain the procedure for library materials preservation both prints and non-prints,
ii. identify the remedies for the treatment of deteriorating library materials;
iii. determine the importance of preservation and
iv. identify the barriers to preservation.

3.0 MAIN CONTENT

Library materials can be preserved through remedial treatment of individual materials, entire materials and stabilisation of the materials to make available for users.

3.1.1 PROCEDURE FOR LIBRARY MATERIAL PRESERVATION (PRINTS)

There are processes through which library materials and systems are maintained, stabilised through preservation procedures. The procedure includes:

- **Controlling the environment:** The atmosphere and environ of the library must be regulated to maintain favourable condition to keep the materials safe from deterioration.
- **Binding of books:** Printed materials normally wane out due to constant or frequent usage. Therefore, it is the responsibility of the Librarians to keep such materials in a usable state by binding or repairing deteriorating ones.
- **Pest control:** Pests like insects, ants, bugs etc are dangerous to the library materials especially the prints resources. The ability to put these pest under control through fumigation and use of insecticides also provides safety for the library materials.
- **Lamination of library materials:** The process of the protection of library materials through lamination involves the coating or sealing of the materials to avoid decay due to frequent usage or rough handling
- **Housekeeping:** A clean environment always is a healthy one. Another way of preserving the library materials is to keep the environment clean from dirt. A dirty environment attracts pests. Therefore, regular sweeping, housework and scrubbing will keep the library and the library materials safe.
- **Adequate ventilation:** It is good to keep the library fresh and airy because inadequate ventilation can affect longevity of the library materials.
- **Handling of materials:** The way library materials are handled determines the level of their good physical condition or otherwise. Rough or unpromising handling of library materials either by librarians or users directly affect them.

3.1.2 PROCEDURE FOR LIBRARY MATERIAL PRESERVATION (NON- PRINTS)

- **Digitalisation:** This is the act of converting information into electronic or digital format that can be accessed by computers or other related devices. This procedure helps in preserving the materials for longer use.

Digital security

- **Sound recording:** It is a process which allows someone to record voice using a microphone and saved as an mp3 file. Most library resources in print and digital format can be preserved through this process. Analog and digital are the two main forms of sound recording.
- **Weeding replacement:** Weeding involves a careful and technical removal of unwanted, old or outdated library materials. Preservation takes place when the newer versions are put in place to replace the weeded materials.

Weeded library print material. https://encrypted-tbn0.gstatic.com

3.2 Remedial treatment of library materials

Part of the tasks of a Librarian is to ensure the correct handling of library materials based on individual materials, the entire collection and stabilisation of library items.

1. **Individual materials:** Remedial treatment of library materials on individual materials bases include:

- Flattening,
- Book and paper repair,
- Binding

2. **Entire collection:** This form involves the treatment of the total collection through:

- Mass deacidication, and
- Fumigation of the library.

3. **Stabilisation:** The process of stabilisation involves the maintenance of the materials and keeping them in a balanced state via:

- Surface cleaning
- Use of new containers
- protective enclosures

3.3 Barriers to preservation

Barriers are the elements or features that prevent or deter the completion of a given exercise or tasks. Barriers to preservation of library materials include:

1. **Lack of disaster/preservation policy**: Some libraries or institutions do not have preservation policy. A policy on preservation acts as guidelines to actions and plans geared towards protecting library materials. The lack of it indicates the failure of preservation of the library materials.
2. **Non-adherence to disaster/preservation policy:** The non-adherence to library preservation policy indicates the presence or availability of the policy or plan which is not being implemented. Consequently, the materials will be vulnerable to agents of deterioration.
3. **Lack of acknowledgement of need of preservation:** It is believed that without making the need for preservation known to the librarians, institutions and the management, there will be lukewarm attitude towards the exercise. Therefore, the need and benefits of preservation must be relayed to all the library stakeholders.
4. **Lack of fund:** The meagre fund and budget of the library always constitute problem to its smooth operations which directly affect the materials preservation and other services rendered by the library. In fact, funds are a major hindrances to every area of library operation.
5. **Lack of personnel and expertise:** Most libraries are short staffed on one hand while some that have enough staff lack the expertise or technical know-how in the preservation and conservation of library materials on another hand.

3.4 IMPORTANCE OF PRESERVATION OF LIBRARY MATERIALS

Preservation exercise in the library is important to the library materials, management, and the users. Enem (2016), highlighted the following importance of preservation:

1. **To restore the material that have already gone bad (decay & damage):** This is bringing back to life some materials that have decayed due to certain agents and also the refurbishment of the mutilated ones to the state where it can be used.
2. **To determine the best appropriate preservation and restoration technique**: The library preservation regulate the suitable procedure, methods, budget and period that preservation should take place.
3. **To prevent those materials that are deteriorating**: Preservation provides the avenue to avoid library material deterioration via repairing, preventing and maintenance of library materials
4. **To justify the budget on preservation**

4.0 SUMMARY

We have looked at preservation of library materials and the security system. Similarly, this unit identified and discussed the various procedures/methods used in preservation of library materials. It highlighted the importance of preservation as well as identified five barriers to preservation of materials which includes lack of preservation policy/plan, non-adherence to existing policy and lack of fund, staff and expertise.

5.0 CONCLUSION

Preservation is concerned with the maintenance and restoration of existing library collections. It is the act of diagnosing and the treatment of library materials. It is also the process of prevention of deterioration, damage and decay to collections in the library.

6.0 TUTORED-MARKED ASSIGNMENT

1. Discuss the procedures involve in the preservation and security of library materials and list five barriers to preservation as discussed under this unit

7.0 REFERENCES/FURTHER READING

Enem, P. (2016) Preservation and conservation of library materials. Retrieved from https://www.bing.com/search?q preservation and conservation of library materials - bing (7th March 2021)

UNIT 4 FACTORS CONTRIBUTING TO THE PHYSICAL VULNERABILITY OF RESOURCES

CONTENTS

1.0 INTRODUCTION

Remember that in this course LIS 307, we have emphasised that as an information manager, you should know that library materials are vital and should be protected and maintained to avoid loss, decay or damage. Hence, preservation is an essential operation in library service. It is therefore crucial for you to know and understand the workings of preservation. This unit explores the factors responsible for the physical vulnerability of library materials and affect the security of the entire library systems. This unit prepares you for your examination and your professional career in librarianship.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to

i. identify the various factors responsible for physical vulnerability of library materials.
ii. identify and explain the reasons for preservation of library materials and apply these strategies to your academic and carrier pursuit to achieve excellent result.

3.0 MAIN CONTENT

Library and information resources have been documented from time to time in a wide range of formats as human knowledge, capability, and skills developed. Initially, it started with cave paintings, papyrus scrolls, handwritten manuscripts, and visual or sound recordings in various languages and formats which provided information to people and allowed knowledge acquired by one generation to pass to the following generation.

Nevertheless, based on some factors, it has not been possible for mankind to save and preserve all the knowledge it has created especially beginning from 14th century which witnessed unprecedented explosion of knowledge and information. This is because some factors have contentiously worked against the institutions which serve as custodians to preserve these range of information from time immemorial.

3.1 Factors responsible for the deterioration of library materials

According to Sahoo (2004), deterioration is a change of original state of any material by interaction between the object and the factors of destruction. The different types of deterioration of the paper-based materials are reflected in wear and tear, shrinkage, cracks, brittleness, warping, bio infestation, discoloration, abrasion, hole, dust and dirt accumulation etc. Some of the factors that make library materials vulnerable to deterioration include-

A. ***Human Factors:*** This has to do with the attitude of library workers as well as the users towards the physical materials in the library. The attitude or actions include: marking with ball pen, dog ear, mutilation, improper storage, deliberate abuse, faulty repair, rough handling, vandalism, folding the fore-edge of pages as a mark of reading.
B. ***Chemical Factors:*** Library materials especially papers are made of fibers with low cellulose content and some other chemical compounds such as alum, rosin. These cause acidic effect and facilitate chemical deterioration of paper as time passes. Also, library materials such as paper usually absorb the moisture chemicals in the atmosphere such as sulphur, oxides of carbon, nitrogen and hydrogen sulphide which expose the materials to deterioration.
C. ***Environmental/Climatic Factors:*** Paper gets deteriorated when exposed to constant/excessive artificial or natural heat and light. In other words, ultraviolet radiation of light and heat are mainly responsible for chemical degradation of paper which takes place when it is exposed to heat and sun in the presence of oxygen. Environmental factors that cause deterioration include light, heat, water, humidity and moisture as well as dust and dirt etc.
D. ***Biological Factors:*** This is also referred to as agent of bio-deterioration. It is usually orgasm that attacks all book components whether paper, leather, straw board, textiles. Hence it is referred to as biological factor because it is caused by biological agent such as

    micro-organisms: fungus, moulds and bacteria

    Insects: silverfish, cockroaches, book worms/beetles, book lice, termites and white ants

    Rodents: mice, rats, squirrels and many other species.

E. Disaster Factors: Generally, in human life, certain sudden calamitous and misfortune occurrence bring great damage, loss or destruction to man and his environment. Indeed, some of these occurrences are due to human error, negligence, mischievousness, or deliberate act. Disaster in library can occur through man-made or natural events. Among man-made disaster are:

War
Fire
Theft

Whereas the natural disaster includes:

Flood
Earthquake
Volcanic eruption
Hurricane

3.2 Reasons for Preservation and Conservation of Library Resources

There is evidence that preservation of library materials dates to several years back. The obvious motive is for easy access and use of the preserved materials when the needs arise.

Popoola (2003) summed up the reasons for the preservation of library resources thus:

1. The society expects libraries to collect and preserve records of the past (such as paper-based materials and other information carriers) in order to learn from them.
2. Library and information resources are expensive to acquire, process and organize for use and should not be allowed deteriorate.
3. Annual library and archive budgetary provisions especially for library resources management have decreased.
4. Library and information resources are essential ingredients for teaching and learning in all educational institutions.
5. The valuable information resources contained in libraries and archives are very useful for development of a country.
6. They are stock in trade and assets of libraries and archives.

Consequently, library management must embark on preservation and conservation programmes for posterity's sake. The process also will safeguard the information resources from fractional and complete deterioration and destruction. In fact, preservation is necessary for the fact that there is the need to meet the ever-increasing information demands of their users. The legitimate and collective tasks of libraries globally make it reasonable for preservation and conservation of information resources

4.0 CONCLUSION

Preservation and conservation of library resources has been in place since the beginning of library services. The rationale for preserving these materials is to fight against the agents that deteriorate or destroy library materials. Therefore, preservation of library materials is a vital tool in conserving and protecting library materials.

6.0 SUMMARY

In this unit, we have discussed the factors of deterioration of library materials which include: human, chemical, environmental/climatic, biological and disaster. Also discussed is that library information and resources are essential ingredients for teaching and learning in all educational institutions which forms one of the reasons for preserving library materials

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. As a contemporary modern librarian, why do you consider it necessary to preserve library materials from deterioration?

7.0 REFERENCES AND FURTHER READING

Popoola, S. O. (2003). *Preservation and conservation of information resources*. Ibadan: Distance Learning Center, University of Ibadan, Ibadan. 3- 4.

Sahoo, J. (2004) Preservation of library materials: Some preventive measures. Retrieved from: https://www.researchgate.net/publication/237645834 (May, 2021)

Unit 5: REPROGRAPHY AND REGENERATION OF LIBRARY INFORMATION RESOURCES

CONTENTS

1.0 INTRODUCTION

This unit introduces you to the process of regeneration and reprography of information resources as a part of preservation mechanism in library service provision. It brings to focus the various types of reprographic services and the role reprography and regeneration play in the preservation process and library service provision, ranging from reproduction and preservation of records, dissemination of information on a large scale among libraries and between libraries and their patrons. The unit also highlights the challenges to reprographic service. The discussion on reprographic service is vital for the fact that proper understanding will help to handle the challenges associated with it as well as enhance preservation of library materials.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. identify the various roles reprography play in preservation of library materials;
ii. identify and discuss the various types of reprographic services available;
iii. recognise the challenges of reprography.

3.0 MAIN CONTENT

To enhance continuity in the provision of library services, the processes of regeneration and reprography of library resources must be established and adhered to. According to Popoola (2008), reprographic services are the reproduction of graphics through mechanical or electrical means, such as photography or xerography.

Historically, Eames Library named after Charles Eames was the first American library to include reprographic package to library services. In 1912, Eames, the then head of Librarians of Lenox Library at the New York Public Library, photo-duplicated rare books, manuscripts, and pamphlets in small editions and distributed them at a normal fee to libraries and historical societies (Udochukwu 2019). Ever since, reprography service has enhanced the use of library materials for the fact that users can now have access to copies of materials even in a situation where somebody is using the original, photocopies could be made for others.

What is Reprography?

The term reprography is derived from two words `Repro' and 'graphy.' Repro means to rewrite or to reproduce whereas `graphy' means printed or written matter. Thus, reprography means reproduction of printed or written matter. It involves processes and methods used for both copy and duplicating (multi-copies) of documents. Reprography is now internationally accepted term which replaces the earlier 'document copying' or 'documentary reproduction'. Reprography includes microcopy (micrographics), photocopy, duplicating and in-house printing. On the other hand, regeneration of information resources in the library is a process which allows the librarian to make duplicate copies of the users' selected document. It is a process where the user and the librarian are not able to edit. It is worthy to note that regeneration and reprography are library terminologies that can be used interchangeably to mean the same

It is in general characterized by the small scale of its operations and the non-professional nature of its operatives. In other words, commercial printing technology is excluded from its scope. Reprography, as explained is a term that is now used in place of photo duplicating, photocopying, duplicating, printing, document reproduction or documentary reproduction (Anyanwu, 2008).

3.1 Role of reprographic services in preservation of library materials

Reprography serves many roles in libraries and these roles amongst others include:

- Dissemination of information on a large scale among libraries and between libraries and their patrons
- Reproduction and preservation of records
- Security of materials
- Storage of important documents
- Securing the protection of information in rare and important texts
- Extensive republications of information of unique collection of data

- Out of print books, manuscript, volumes of periodicals
- Saving of space in the library.
- Helping in the preservation and conservation of library materials.
- Assisting in the reproduction of rare books, of print and archival materials for the purposes of storage and use.
- Promoting inter-library corporation resources and sharing and
- Enhancing the use of library materials and facilitating the reproduction of exact copies of document.

Reprography, the science of duplicating printed matter through such methods as microfilming and photocopying, has been used in libraries for over a century. Methods of reprography have included microphotography, microfilming, Photostatting/photographing, and xerography, amongst others.

3.2 Types of Reprographic Services

Reprographic services encompass such services that aim at making printed materials more easily available such as: xerography, microscopy, photocopy, duplication and in-plant printing

1 **Xerographic printing:** This involves a photographic process that is completely dry, using no solutions or fumes, and permanent copies can be produced from the original document within a few minutes.

Xerox printing. Source: https://www.google.com/search

1. **Photocopy:** This reprographic service makes a photographic reproduction of graphic or printed materials. It is a form of making copies of required items from books, journals, newspapers or pamphlets etc. It is a very valuable service to the library patrons. Photocopying (in broader sense, any kind of machine reproduction) comes under the provisions of copyright and affects the document supply services of libraries and information centres.

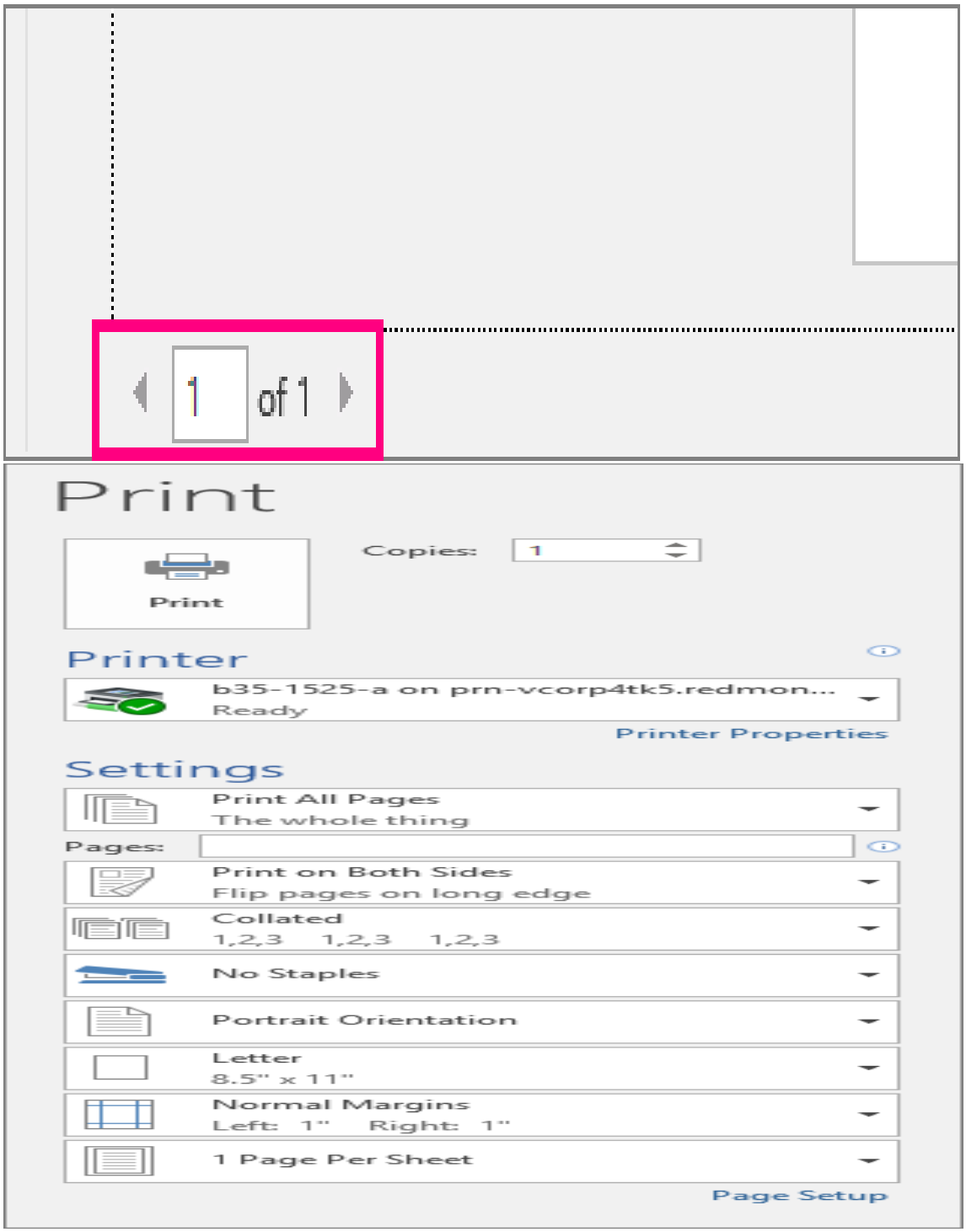
Photocopying and printing services is available in all our libraries. It is important to know that the Copyright Act allows anyone to photocopy works without securing permission from the copyright owner when the photocopying amounts to a "fair use" of the material. There are guidelines that give the boundaries for fair use of photocopied materials used in research and academic works.

Photocopying' Source: machine
https://www.collinsdictionary.com

2. **Duplicating:** The process of making a copy out of print material like the original.

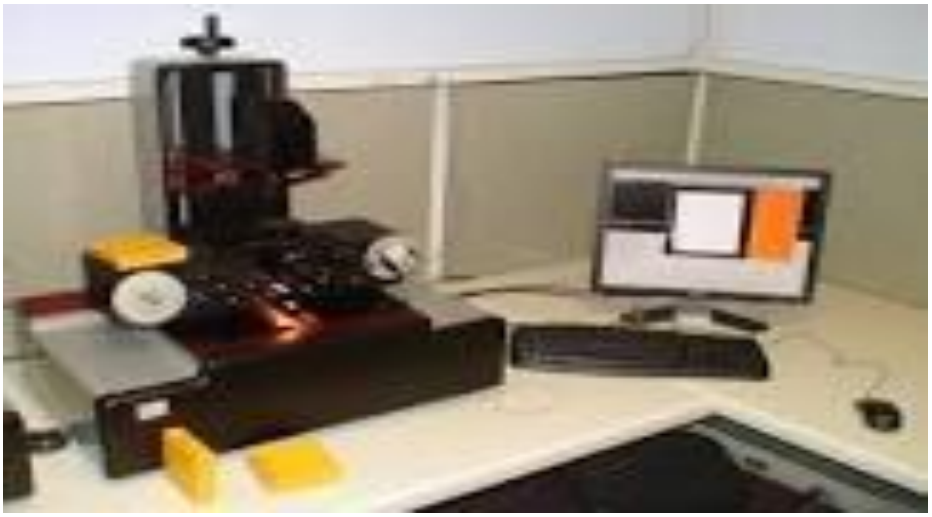
Duplicating material Sources
https://history.churchofjesuschrist.org

3. **In-plant printing (Office printing):** This form of reprographic service enables the library to reproduce or regenerate library and information resources by printing out the documents from the original. It follows the process of previewing the document in the system, specifying the particular page(s) you want to print and printing.



In-print format. Source: https://files.support.epson.comn

4. **Microfilm:** The microfilm is a morphography of cellulose film. It is a planetary camera popularly used in the library for reprographic services. It is a 35mm of 16mm still camera mounted on a vertical column that take about 100ft of film at a loading and it can photograph single sheets of books.



Microfilm: Source: https://en.wikipedia.org/wiki/Microform

3.3 Challenges to Reprographic Services

Several issues are militating against the effective provision and utilisation of reprographic services by the library, librarians and library users especially in the third world countries. These include:

1. Non-availability of the reprographic equipment within the library
2. Poor maintenance culture of the library management towards the equipment
3. Inadequacy of fund to buy, replace or refurbish available equipment
4. Lack of trained manpower to operate, maintain and drive the equipment

4.0 CONCLUSION

The provision of reprographic of information resources is among the services in the library is vital and provides the users the opportunity of access to a range of information resources which are usually limited in number. In addition, reprographic services also serve as preservation and conservation mechanism to the library materials

5.0 SUMMARY

In this unit, examined the meaning of reprographic service in the library and the various types which include: xerox printing, microscopy, photocopying, microfilms, duplicating, and in-printing among others. We also discussed the role of reprographic services as well as the challenges confronting reprography and regeneration of information resources.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. List and explain the factors challenging the provision of reprographic services in the library.
2. What significant role does reprography play in the provision of library services

7.0 REFERENCES AND FURTHER READING

Popoola, S. O. (2003). *Preservation and conservation of information resources*. Ibadan: Distance Learning Centre, University of Ibadan, Ibadan

Udochukwu, D. (2019). Reprographic services: availability and effective accessibility of university library materials by students in Enugu State University of Science and Technology, Retrieved from htpps://digitalcommons.unl.edu/libphilprac (18th May 2021)

MODULE 3 INFORMATION SECURITY

This module will be discussed under the following units:

Unit 1 Information Security and library services

Unit 2 Cryptology and network security

Unit 3 Issues in information security

Unit 4 Software security and authentic protocol

Unit 5: Principles and network security for preserving, conserving and security library items

UNIT 1: INFORMATION SECURITY (*INFOSEC) IN* LIBRARY

CONTENTS

1.0 INTRODUCTION

Information security, also called *infosec* is a central concern in libraries of all kinds. It is imperative for libraries to take deliberate steps to secure all their book and non-book items. Without adequate efforts, techniques and tools to secure library and information resources, there would be loss, damage, mutilation and destruction of valuable and highly prized materials. In fact, libraries have suffered tremendous damage to their collections. Therefore, it is necessary to examine all the implications of infosec in library and information centres. It is important to note that adequate security measures to protect library resources will enhance efficient service delivery.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. ascertain the meaning and the scholarly use of information security in the library.

ii. identify the mechanics of securing library items and how to apply them.
iii. determine the principles of information security and how they work

3.0 MAIN CONTENT

The word 'security' is derived from the Latin word '*secures*' which literally means 'free from danger'. In other words, the state of being secured. According to Fischer and Green (1998), security implies a stable, relatively predictable environment in which an individual or group may pursue an end without disruption or harm and without fear of any disturbance or injury.

3.1 Information Security '*Infosec'*

What is Information Security?

Information Security is a set of practices intended to keep data secure from unauthorized access or alterations. Here's a broad look at the policies, principles, and people used to protect data. This module on information security will introduce you to the concept of cryptology and network security, issues in information security as well as access control and external attack on information resources.

In today's world, information creation, use and dissemination has become a valuable asset. Therefore, the need to secure whatever information generated has become necessary and this has given rise to the concept of information security 'i*nfosec'*. Information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption (SANS, 2020).

Generally, security involves safeguarding and prevention for safety. It can also be seen as freedom from attack and potential harm from others. Information security has therefore become the process or measure of protection against unauthorised access and use of the information or data weather in print or electronics format. There are many definitions of information security - *infosec*. In essence, different scholars have defined it according to their discipline and school of thought.

According to Fruhlinger (2020), information security is a set of practices intended to keep data secured from unauthorised access or alteration, both when it is being stored and when it's being transmitted from one machine or physical location to another. Information security might as well be referred to as data security. It is obvious that knowledge has become one of the 21st century's important assets. Therefore, efforts to keep them secured have correspondingly become increasingly important. According

to CSRC (2019) the term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability.

3.2 Principles of Information Security

An institution that uses computers and other information bearing electronic devices ought to know and describe their information security needs as well as trust the system in which the security of the information will be built on. To secure a formidable information security, players and owners of the information as a matter of fact must adhere to the required basic principles. The three major principles/requirements of information security process include:

D. ***Confidentiality:*** This has to do with maintaining the privacy and secrecy of information or data and also having a firm control of its access and use.

E. ***Integrity:*** This type of requirement deals with the ability to ensure that information and programs do not change without the authority of the institution or individual that owns it. This means that change can only come in a specific and approved manner.

F. ***Availability:*** The principle of availability ensures that only authorised users get continual access to the available information and resource in the system.

4.0 CONCLUSION

Preservation and conversation of information material have been a problem that has to a large extent affected the smooth running of library services. The advancement of information and communication technology has brought about proliferation of information in abundance which has overwhelmed librarians and other information managers. It is the responsibility of the libraries and librarians to ensure information resources and other materials in the library are well organised and preserved for longevity and easy access and use.

5.0 SUMMARY

In this unit, we discussed the concepts of preservation, conservation and information security - *infosec*. Similarly, we examined the techniques of preservation and the threats to information resources and library materials, and the principles of information security which include, confidentiality, integrity and availability.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. Mention and explain the three characteristics on which the principles of information security are built?

7.0 REFERENCES AND FURTHER READING

Computer Security Resource Center (CSRC) (2019) *Cybersecurity Supply Chain Risk Management.* Accessed from**:** https://csrc.nist.rip/ (4th January 2021)

Fruhlinger, J. (2020) Information security and practices Retrieved from https://www.sans.org/information-security (6th March 2021)

IFLA (2010) Principles for the care and handling of library materials international preservation issues, Retrieved from http://archive.ifla.org/VI/news/pchlm.pdf. (8th March 2021)

SANS (2006) Information security. Retrieved from https://www.sans.org/information-security/ (4th April 2021)

UNIT 2 CRYPTOLOGY AND NETWORK SECURITY

CONTENTS

1.0 INTRODUCTION

The focus of our discussion in this is on cryptology and network security as it relates to library operations. We will also discuss the differences between cryptology and network security and how both work in the provision of library services.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

At the end of this unit, you are expected to:

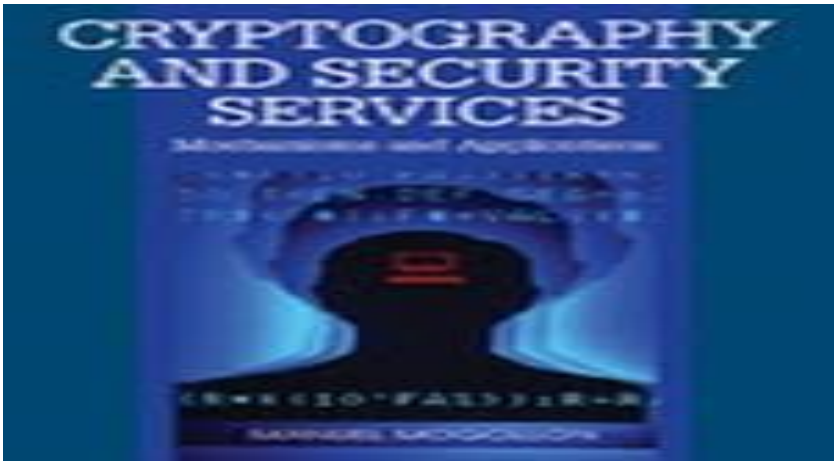
i. explain the meaning of cryptology and network security
ii. identify the various types of cryptography
iii. analyse the roles cryptography play in the preservation of library materials
iv. identify the information some of the existing library security policy and measures

3.0 MAIN CONTENT

Information or data repeatedly travels from one computer to another and from network to network exposing the security and threat of the contents. As soon as the data is out of hand, it is exposed to interference and hacking. Hackers can intercept the data either for amusement or for

personal benefit. Hence, the idea of cryptography is to reformat and transform our data, making it safer on its trip between computers and networks. The technology behind cryptology is based on the basics of secret codes, augmented by modern mathematics that protects our data in powerful ways.

Earlier, cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice

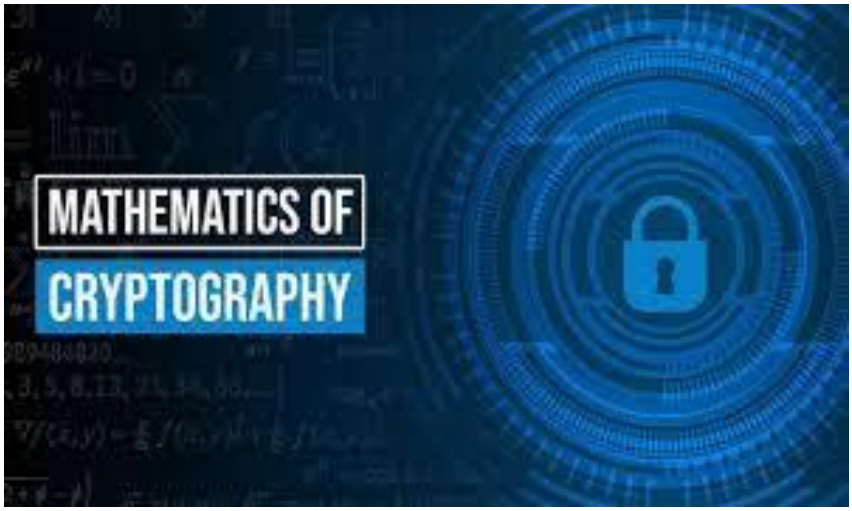


Cryptography and security services: Source *https://sectigostore.com*

3.1 Definition and Meaning of Cryptology?

According to an online definition, cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication.
Also, cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word ‘cryptos’, which means hidden.

Furthermore, Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis. To do this, certain mathematical equations are used, which are very difficult to solve unless certain strict criteria are met.



Cryptography Source:
https://www.youtube.com/watch?v=uNzaMrcuTM0

Simmons (nd) defines cryptology as a science concerned with data communication and storage in secure and usually secret form. According to him, cryptology encompasses both cryptography and cryptanalysis.

Cryptology has two components, cryptos and logos. Cryptographic methods to certify the safety and security of communication and main goal is user authentication, data authentication such as integrity and authentication, non-repudiation of origin, and confidentiality and it has two functions - encryption and decryption.

3.2 Basic Concepts in Cryptology

Cryptography: The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

Plaintext: The original intelligible message

Cipher text: The transformed message

Cipher: An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Key: Some critical information used by the cipher, known only to the sender& receiver

Encipher (encode): The process of converting plaintext to cipher text using a cipher and a key

Decipher (decode): The process of converting cipher text back into plaintext using a cipher and a key

Cryptanalysis: The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking

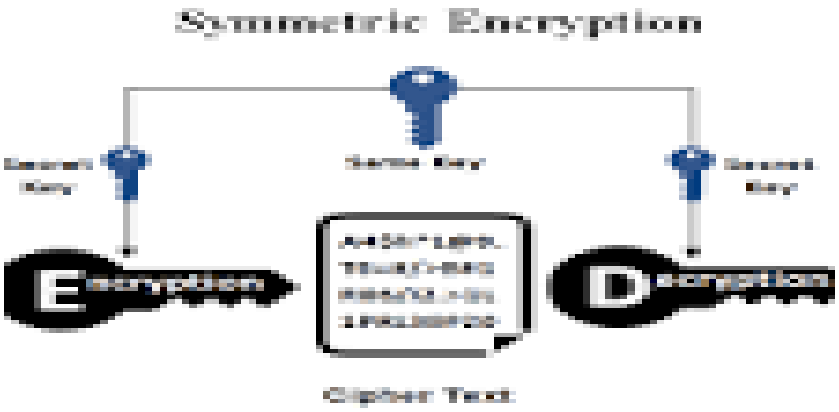
Cryptology: Both cryptography and cryptanalysis

Code: An algorithm for transforming an intelligible message into an unintelligible one using a codebook.

3.3 Types of Cryptographs

There are three common types of cryptography, and these include:

1. **Secret/Symmetric Key:** This type of cryptography uses single key for both the sender and the receiver (i.e. single key for encryption and decryption). The sender and the receiver know the same secret code. Therefore, the sender encrypts the message and the receiver decrypts it with the singular secret code that is known to both. Secret key cryptography use is such as data encryption standard, advance encryption standard, Cast-128/256, international data encryption algorithm, and rivets ciphers etc. (Citrix-system, 2010).



Symmetric encryption: Source: https://www.ssl2buy.com/wiki/symmetric

2. **Public/Asymmetric Key:** This type of cryptography involves the use of couple of keys for encryption and another for decryption. The key work in pairs of coordination - public and private keys. Public key can freely distribute the private key. If senders and receivers don't have to communicate keys openly, they can give private key to communicate confidentially. Public key cryptography can be used for key exchange and digital signatures such as RSA, digital signature algorithm, public-key cryptography standard etc.
3. **Hash Function:** This can also be referred to as message digests which has one way encryption. The high function key type of cryptography

involves the use of a mathematical conversion to permanently code information. Hash function use to provide a digital fingerprint of file contents and it is commonly employed by many operating systems to encrypt passwords and it provides a measure of the integrity of a file. It also uses message digest, secure hash algorithm, RIPEMD etc. (Kessler, 2010).

3.4 The Role of Cryptography

The network security has become a great concern to the information managers both in academic and business world especially with the growth of ICT, the Internet and other computer related information resources. Hence, the need to involve cryptography technology system to checkmate information arises.

Cryptographic image Source: www.informationage.com

There are five basic roles that cryptography play in securing information and these include:

1. **Access Control:** This is an admittance regulation whereby only the authorized person(s) can login & password (key) to access the confidential data/information.
2. **Confidentiality:** Concealing information from unauthorised access and use by hiding the message via a cryptographic key
3. **Integrity**: Cryptographic tools give integrity that permits a recipient to authenticate that the message is transformed and cannot prevent a message from being transformed but effective to identify either planned or unplanned change of the message.

4. **Authentication**: The ability to verify who sent a message. It is done through the control key because those with access to the key can encrypt a message.
5. **Hash function**: The high function of cryptography in securing information involves actions such as digital signature and providing message authentic code(s). This cryptographic function uses different methods to certify that the message is not changed or altered.

3.5 Guide to Safety and Security of Wireless Network Security System

In today's world, ICT and wireless networking systems have become common and have paved the way for computers to connect without the use of physical cables. It has also made the use of internet connectivity easier, more convenient and faster through the use of computer connections via devices such as Wi-Fi /802.11, wireless routers and surf internet to print documents, download materials, transfer messages and data as well as email. On the other hand, it has also provided an avenue for cyber theft, and outsiders/hackers to have access and use of information ordinarily not meant for them.

Wireless security network Source: https://www.kaspersky.com

Hence, the following are the tips to guide and keep wireless network security system safe and secure thus:

- Keep-out undesirable wireless guests: only those who can access with right password or encryption key and restrict wireless network to normal office hours.
- Choose strong password – Where possible password should be longer (20 characters) it takes someone to figure it out; Use mixture lowercase and uppercase letters; Insert numbers in between letters;
- Change password every 3 months;

- Write password down and keep in safe place (in case of forgetfulness).
- Use the firewall – it is front security and secures network, computers and data from snooping eyes;
- Don't show the name of the network (SSID);
- Change default SSID, don't use name to identify the organisation;
- Use MAC filtering because each network card is a unique code known as MAC address and access points to restrict access to only the authorized.
- Switch on and use built-in encryption to prevent eavesdrop.
- Restrict user ability (network administrators) to setup quick and dirty wireless network, even temporarily. One rogue access point can undo all the good work you do on the others.
- Certify all security measures are in place, its result is defense against intruders;
- Turn off the wireless network when it is not in use.
- Hide/keep safe place confidential files/data (Microsoft, 2010; Bryan, 2010)

3.6 Information Security Policy

Security policy. Source: *www.kaspersky.com*

Generally, a policy is a statement embracing the general goals and acceptable procedures and guides for achieving the set objectives. A library or any other organisation without a policy guiding its actions and inactions especially as it relates to security are bound to expose its useful

information to outsiders and hackers. Hence, information security policy must include the following among others:

- A statement describing the purpose of the *infosec* program and overall objectives
- Definitions of key terms used in the document to ensure shared understanding
- An access control policy, determining who has access to what data and how they can establish their rights
- A password policy
- A data support and operations plan to ensure that data is always available to those who need it
- Employee roles and responsibilities when it comes to safeguarding data, including who is ultimately responsible for information security (Fruhlinger 2020)

3.7 Information Security Measures

Information security measures are various security checks applied by an organisation/institution to regulate unauthorised access and use of codified information/data by persons or group of persons. These include:

1. **Organisational measures:** This measure has to do with the deliberate establishment of internal security structure committed to the organisation's security in addition to co-opting part of different departments into *infosec.*
2. **Human measures**: Capacity build and coaching of personnel on appropriate *infosec* uses and practices
3. **Physical measures:** Deals with access control to the office locations, premises and, especially, data centres
4. **Technical measures**: This is the hardware and software that protects data — everything from encryption to firewalls

Security measure. Source:www.technologyreview.com

4.0 CONCLUSION

The importance of information security and network cannot be over emphasised for the fact that without adequate security vital information is either lost or may get into a wrong hand. It is worth noting that security is a set of practices intended to keep data secure from unauthorized access or alterations. Therefore, there is need to create the policies, principles, and the personnel charged with the responsibility of using information/data and protecting same.

5.0 SUMMARY

In this unit, you have been exposed to cryptology and security network. Accordingly, we saw cryptology as a science concerned with data communication and storage in secure and usually secret form. some of the areas discussed in cryptology such include:

- Basic concepts,
- Principles of Information Security
- Types of cryptography,
- The Role of Cryptography
- Tips to guide and keep wireless network security system safe and secure
- Information Security Policy
- Information security measures

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. List and explain the four measures mentioned in information security.
2. What are the issues to be considered before formulating information security policy?
3. Discuss the role of cryptography in information security?

7.0 REFERENCES AND FURTHER READING

Brian, G. (2017) Keep your window computer secure on public wireless hotspots. https://www.howtogeek.com/

Chandrasekhar, D. R., Kumar, A, R., & Kabat, M. R. (nd) Cryptography and network security lecture notes. Retrieved from www.cryptologyandsecuritynetwork.com/pdf (19th May,2021)

Fruhlinger, J. (2020). What is information security? Definition, principles, and jobs. Retrieved from https://www.csoonline.com/article/3513899/.html (4th June 2021)

Kessler, G. & Bikowski, D. (2010), Developing collaborative autonomous learning abilities in computer mediated language

learning: Attention to meaning among students in wiki space. Computer Assisted Language Learning, 23 (1): 41-58.

Microsoft (2010) Introduction to Access 2010 security. https://support.microsoft.com/en

Simmons, J. (nd) What is Cryptography. Retrieved from https://economictimes.indiatimes.com/definition/cryptography (19th June 2021)

UKEssays. (November 2018). The role of Cryptography in network security computer science essay. Retrieved from https://www.ukessays.com (1st June 2021)

UNIT 3 ISSUES IN INFORMATION SECURITY

CONTENTS

1.0 INTRODUCTION

This unit examines the issues in information security *infosec* such as firstly, physical issues which include site design, building design, security personnel, burglary, theft, vandalism etc., as well as electronic issues which include cyber theft, hacking etc. Our discussion will also to how to maintain information security especially in the library.

INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. identify the physical issues relating to information security;
ii. recognise the cyber related security issues**;**
iii. explain ways to maintain information security in the library and apply the strategies.

.

3.0 MAIN CONTENT

The library, librarians and library services have witnessed and still undergoing several changes in recent times. These changes are poised to meet the information needs of the users and the changing world. The library is striving to get acquainted with the ever-improving information and communication technologies (ICT) in automated librarianship and most importantly, the information security associated with it. According to Gupta and Madhusuhan (2018), although the quest for better security for the library material and its environment has always been the primary

concern, the introduction of ICT has increased the risks and challenges manyfold.

Network security threat. Sources: https://encrypted-tbn0.gstatic.com

Security issues in the library will be discussed in two dimensions namely:

Physical (non-electronic) and cyber security issues

3.1 Physical Security Issues

Site design: The proper security starts with the physical arrangement of the environment and the surrounding ensuring conducive atmosphere as well as supporting appropriate surveillance, but this is not always the case in some libraries where location or spot are not considered before situating a library thereby increasing the security risk.

Building design: Most libraries building today lack the basic architectural design meant for library because they were not originally designed to be a library, rather they are converted buildings thereby creating security loophole. On the other hand, an ideal building design of the library and its facilities should contain a model architectural design such as an access control mechanism whereby the movement of the library materials, users, staff and visitors are carefully monitored to avoid resource/materials loss or theft.

Security Personnel: Most libraries lack professional and well-trained security workforce who ought to be on regular guard and patrol to protect library building, facilities and the resources therein at all times.

Window/Door protection: The entry and exit points as well as the window meant for ventilation if not well protected, most times exposes the vulnerability of library and her materials.

Burglary proof: The lack of break-in or theft protection in the library used to safeguard the windows, doors, manholes and other openings created an opportunity for the loss and theft of materials in the library.

Theft and mutilation: Regular loss of library materials due to stealing by the supposedly library users create a big security issue. In addition, the frequent mutilation in a way of malicious dismemberment of library materials especially prints resources constitute other issues to the library and the resources.

Vandalism: This is an act of sabotage and intentional damage to the library, the building, facilities and resources. Vandalism is an intentional act of destruction or defacement of another person's property. It happens usually during a socio-political unrest.

Disruptive behaviour: Disorderly conduct of some patrons can cause security breach in the library. For instance, some users may be acting under the influence of alcohol or other intoxicated substances to cause security problems.

Damage and disaster: These are occurrences which can destroy the physical library and large volumes of library resources. According to Aziagba and Edet, (2008) another problem of security of library materials is disasters that threaten the collections. "Disasters can be natural as well as man-made. There is little or no control over natural disasters, which come usually as a result of flood, landslides, earthquake, storm, cyclone, or hurricane. Whereas man-made disasters are caused mostly by human negligence such as fire, leaking roof etc.

3.2 Cyber Security Issues

Globally, cyber-crime has become a major security challenge to the governments, corporate organisations, institutions, individuals, the library etc. It can be argued that the proliferation, availability and easy access to internet connection has created countless security lapses and exposure of vital information to unauthorized persons.

Cyber Security: ***www.thesslstore.com***

The following are the issues associated with cyber security:

Cyber Theft: The act of impersonation and accessing someone's' identity for online criminal activity usually through phishing. ***Phishing*** involves creating fake websites that look like legitimate business websites or emails and the use of fake Wi-Fi hotspots that look like legitimate ones.

Hacking: Hacking is used to by-pass security controls to gain unauthorized access to a system. As soon as attackers gain access to the system, they can install programs that allow the attackers to spy on the user or control their system remotely, steal sensitive information and deface websites

Computer viruses: Viruses are malicious and unauthorized programs that can annoy users, steal sensitive data, or be used to control equipment that is controlled by computers

Unauthorized access: where hackers, intruders and attackers could have the privilege of accessing unauthorised information through any dubious means by circumventing the standard convention such as username and password.

Data loss – This form of security issue occurs when data collection centre or office is engulfed by fire or flooded with rainwater or other disaster agents and the stored data is damaged or lost.

Copyright infringement: This is the act of infringement to the unauthorised use of copyrighted materials**.** The effort to maintain privacy, confidentiality and integrity of information from the original owner has remained a major security issue today. This is because fast internet access and reducing costs of storage have contributed to the growth of copyright infringement crimes.

Cyber infringement: www.thesslstore.com

3.3 How to Maintain Information Security in the Library

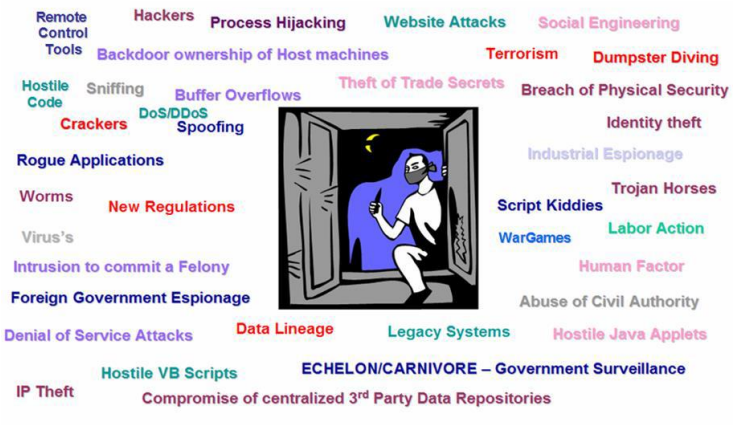
The number of library users and their activities are increasing progressively. This has put more pressure on the librarians and facilities as well as the materials which leads to increased exposure to more security issues. Despite the numerous information security issues mentioned, there are physical and electronic systems that can be employed to checkmate and protect these materials. They include:

3.3.1 Physical Security Checks

3. **Serene Environment:** Proper security starts with the physical arrangement of the environment and the surrounding ensuring conducive atmosphere as well as supporting appropriate security surveillance.
4. **Security personnel:** The security personnel should be employed to undertake patrol within the library and to enforce appropriate library access at the main lobby. Inspection of bags and other belongings of library users while entering and leaving the library by security/library staff should be practiced.
5. **Regular repair work**: A steady repair of broken windows, doors, to check unauthorised access and check burglary. In addition, consistence repair of damaged lighting point, water pipes and leaking roof as well as other facilities to prevent damage to the library building and materials. Provision of cheaper facilities for photocopying in libraries to discourage and prevent stealing and

mutilation of library print materials. For instance, when a user knows that he/she can make a cheap photocopy of a print material within the library he/she will reject the temptation of stealing and/or mutilating library materials.

Installation of Collection protection device: Collection detection device is placed on the library materials such as books, magazines, video cassettes, audio cassettes, CDs and DVDs as well as a detection device that is typically located at a library exit. The detection device must be safe for magnetic media, usually with audible/or visible alarms; if desired, the audible alarm can be voice alarm. According to Brown and Patkus (2003), "there are two major methods currently used for detection: *electromagnetic* and Radio Frequency Identification *(RFID)* RFID.



Counter security: http://eprints.covenantuniversity.edu.ng

6. **Video Surveillance Cameras:** A device such as Closed-Circuit Television **(CCTV)** is video surveillance system. It serves the purpose of secretly monitoring and recording the movement of persons and materials in and outside the library building. It deters crime and ensures safety. McCahill and Norris (2002) noted that libraries can use CCTV to identify visitors and employees, monitor work areas, deter theft and ensure the security of the covered areas. It can also be used to monitor and record evidence on clientele and staff misconduct in the library. The device can be used to:

- monitor corners of the library building,
- driveway to the library,
- parking areas,
- delivery points,
- shelf areas,
- staff and users' movement,
- library activities such as exchange of materials and
- equipment such as computers etc.

CCTV Camera. Source https://upload.wikimedia.org

3.2.2 Cyber Security Check

Nowadays, the use of computers connected to the internet has exposed individuals, institutions, government and libraries etc to cyber security threats. The illegal activities by unscrupulous individuals are designed to harm, steal, manipulate and hack as well as rob individuals or groups of their sensitive information for malicious reasons. This is achieved by simply knowing the password to the email IDs or other social networking accounts of others. Eldard (2016) listed 8 internet security tips to maintain security thus:

1. **Always have an Antivirus**: Antivirus is a software designed to identify and destroy computer viruses in your system. Antiviruses are meant to defend your computer from being attacked by virus, malware, adware, spyware etc.
2. **Do not download stuff randomly:** Despite installing antivirus, it is wise to always verify every software you want to download to ascertain its origin. This is because some software are there to steal sensitive information from unsuspected downloaders.
3. **Update software regularly**: This is done to replace the older version with the new ones. It is advisable to use the antivirus that has the latest antivirus software to update from the outdated to the latest version.
4. **Use safe browsers:** The reliable browsers are built with internet security in mind by the developers. They will encrypt your information, allow you to enter information automatically and inform you if you are on a website that is not safe for providing your confidential information. You can use such browsers for your daily tasks too if you want to.

5. **Do not click on unknown links:** Some unsubscribed or unknown emails are scam even though they look real. Hackers and attackers employ this style to have access to their victims' email or social networking account.
6. **Always check SSL information:** In order to play safe while providing your personal or confidential information to a second party, make sure you are on a HTTPS link and not an HTTP link on some websites. These security layers ensure that all the information you provide will be encrypted on the website and no third party can access it
7. **Scan external storage devices:** Obviously, external storage devices such as flash drives are the major carriers of viruses and other security compromising software. The best way to keep away from this threat is to have your antivirus on auto scan settings
8. **Don't rely on trial Antivirus versions:** Trial and demo antiviruses are not the original antivirus versions. Therefore, they cannot protect your computer from internet threat. It is better to use reliable cyber security consultancy services to help you secure all your computers as well as the network they are connected on (Eldard, 2016).

Information system security. Source: www.guru99.com

Other ways of maintaining secured cyber information security include:

1. **Biometric Identification:** Used to control unauthorised access. It is designed in a way that it can record the user's fingerprint and use it for authentication purposes which is

aimed at stopping unauthorised persons from gaining access.

Biometric device. Source: www.bayometric.com

2. **Data backups:** This is considered the best standard security practice. Institutions, organisations even individuals keep backups of the data at remote places. The data backups are kept to bring relief in case of occurrence of any form of disaster. The backups are made periodically and are usually put in more than one remote area.

4.0 CONCLUSION

The issues in information security are a vital concern in library services. It is the act of identifying and preferring the solution that deals with the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability. Information security is a process for the fact that it is a journey not a destination. This is because there will always be new ways of doing things, new threats, new vulnerability, new modalities, new technologies and new counter measure to information security.

5.0 SUMMARY

Every library in the world is faced with issues associated with the security of information resources and materials. Some of the issues of concern in information security are categorised into two broad dimensions: physical and cyber issues. These concerns can be combated through physical and cyber means available for maintaining information security in the library.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. List and explain the tips in maintaining cyber information security.
2. Explain the physical issues in information security?
3. Highlight the cyber issues in information security?

7.0 REFERENCES AND FURTHER READING

Aziagba, P. C. & Edet, G. T. (2008). Disaster control planning for academic libraries in West Africa. *The Journal of Academic Librarianship, Vol.34*, no.3: 265-268.

Brown, K. E. & Patkus, B. L. (2007). *Collection security: Planning and prevention for libraries and archives*. Northeast: Document Conservation Centre.

Eldard, K. (2016) 8 outstanding ways to maintain your cyber security. Retrieved from https://www.buzzfeed.com/kimeldard (6th April 2021)

Gupta, P. & Madusudhan, M (2018) Security of library materials: challenges and solution Retrieved from http://www.nedcc.org/resources/leaflets/3Emergencymanagement/11collectionsSecurity.php . (17th June 2021)

McCahill, M. & Norris, C. (2002) - Center for criminology and criminal justice …, Retrieved from www.urbaneye.net 6th April 2021)

Omosekejimi, A. F., Ijiekhuamhen, O. P. & Ojeme, T. N. (2015). Library and information resources security: Traditional and electronic security measures.

Retrieved from https://www.idpublications.org (3r June 2021)

UNIT 4 SECURITY SOFTWARE AND PROCEDURE

CONTENTS

1.0 INTRODUCTION

Our discussion in this unit centres on software security and authentic protocols. The software packages include applications and documents that are information carrying devices which can be corrupt while in the storage and during transit whereas authentic protocol is a form of computer communication and cryptographic protocol that is designed specifically for the transfer of authentication data between two entities. We will also examine the difference approaches, guidelines, standards, policies and procedures as well as steps in achieving operational and organisational security.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. explain and analyse the concept of software security and authentic protocol;
ii. identify the various forms of software security;
iii. recognise the software security, lifecycle
iv. identify the possible solution to the challenges of information security and the how to apply the solution strategies

3.0 MAIN CONTENT

Normally, a software security is intended to secure and protect networks, laptops, servers as well as mobile devices from threats, intrusions, viruses and unauthorized persons. It is also designed to proffer defence to computer users, data, companies and systems from a wide range of threats. Presently, users or organisations operating without information security software or using an outdated security software stand the risk of exposing the system to a wide range of threats such as viruses, hackers, malware and spyware.

At present, due to ever increasing sophistication and diversity of cyber threats and growing figures of endpoints that need protection due to an increase in mobility, remote work and the Internet of Things (IoT). This has necessitated many organisations to employ ever more innovative security software solutions to arrest the advancing security threats.

Internet of things (IoT). Source: www.zdnet.com

3.1 Software Security

What is Software Security?

Though software security may be regarded as a new concept, yet its definition varies especially in applications, designs, disciplines and among scholars

Cyber Security reciprocity.com

The Dictionary of Cybersecurity defines software security as an idea implemented to protect software against malicious attacks and other hacker risks so that the software continues to function correctly under such potential risks. Security is necessary to provide integrity, authentication and availability (Technopedia 2021).

According to Forcha (2020) software security is the building of secure software with inherent defence so that it continues to function under malicious attacks, to the satisfaction of the users and owners of the software. What is secured is information and software packages (applications and documents). Information is any message that is useful to anybody. "Information" is a vague word. The context in which it is used gives its meaning. It can mean news, lecture, tutorial (or lesson), or solution. A software package is usually a solution to some problems. In the past, all information not spoken was written on paper. Today, the software can be considered as a subset of information (Forcha, 2020).

According to the Information Security for South Africa (ISSA), computer security software or cybersecurity software is any computer program designed to influence information security. This is often taken in the context of defending computer systems or data. However, it can incorporate programs designed specifically for subverting computer systems due to their significant overlap, and the adage that the best defence is a good offense (ISSA, 2011).

Central information security monitoring unit. Source: www.evansonline.com

The advancement in technologies has made information security an important task in computer communication networks. Recently, security devices were facing challenges in dealing with network threats posed by attacks. Consequently, software definition of security (SDS or SDSec) has been recommended to counter these challenges. It is a model in which information security is controlled and managed by security software. The

functions of network devices such as firewalling, intrusion detection, access control and network segmentation are extracted from hardware device to software layer. This software is used to control and manage resources. Protection is based on logical policies, not yet to any security device. (Sadiku, Shadare, Koay & Musa, 2016)

Videolink: https://www.bing.com/videos

3.1.1 Ways to Software Security Practice

Johnson (2020) listed some tips to follow to enhance the best software security practices and these include:

- Learning the level of sensitivity of the information to be handled by the program and in the system
- Classifying the information
- Making sure all the sensitive information is properly encrypted
- Taking advantage of the most secure and reliable providers when using third-party libraries.
- Paying as much attention as possible to authentication and its levels.
- Taking a serious approach to training on app security including network, endpoint and content security.
- Building control at each of the access point based on the specific needs of the users.
- Testing the program for the security violation,

3.2 Forms of security software programs

Institutions, organisations and individuals at different points in time employ different security software programs/applications to monitor and/or protect their sensitive information from unauthorised use and access. CISC (2020) mentioned some of the leading examples of security software programs/applications to include:

Advanced malware protection software: This form of security software is designed in a well-organized way to detect, avert as well as help remove threats like software viruses and other malware such as ransomware, worms, Trojans, spyware, adware, and fileless malware from computer systems. It is a security solution that addresses the full lifecycle of the advanced malware problem. It prevents breaches and gives the visibility, context, and control needed to rapidly detect, contain, and remediate threats if they evade frontline defences.

Application security software: To secure adequate information security, an institution needs to apply a wide range of applications that will help to monitor the applications running in their environment, its activity and most importantly who is accessing the applications. Application security (short AppSec) includes all tasks that introduce a secure software development life cycle to development teams. Its final goal is to improve security practices and, through that, to find, fix and preferably prevent security issues within applications. It encompasses the whole application life cycle from requirements analysis, design, implementation, verification as well as maintenance.

Firewall software: This security software compares networks behaviour to potential threats by tracking them. It is a security software that can send notifications if it detects changes to security policy or potential vulnerabilities created by policy change. It has the potential to prevent unauthorized access to or from private networks. Firewalls can also be hardware, and firewall software and hardware are often used together.

Endpoint security software: Endpoint protection systems are designed to quickly detect, analyse, block, and contain attacks in progress. The systems need to collaborate with each other, and with other security technologies, to give administrators visibility into advanced threats to speed detection and remediation response times.

This type of software helps to protect the data and workflows related to the various devices--such as laptops, smartphones, and tablets that connect to a corporate network. Endpoint security combines preventative protection with a new breed of continuous detection and response capabilities. Using cloud-based analytics, it eliminates bloated agents from consuming valuable CPU resources.

Web security software: Web security software can monitor inbound and outbound network movement to help decrease the risk of sensitive data theft or leakage. It can also offer protection from zero-day threats (threats that leverages unknown vulnerabilities).

Network security software: Network security software helps users detect and stop unauthorized network access due to phishing, spyware, and more. It can also help to protect data in transit and at rest. Network security solutions include:

(i) Identity and access management (IAM). IT administrators use IAM solutions to manage users' digital identities and related access privileges securely and effectively. They can set up and modify user roles, track and report on user activity, and more to protect data security and privacy.

(ii) Next-generation IPS (NGIPS). NGIPS threat appliances provide network visibility, security intelligence, automation, and advanced threat protection. They can

inspect the network perimeter, and they can track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

(iii) Security Information and Event Management (SIEM). Many organisations use SIEM products for real-time reporting and long-term analysis of security events. These products include physical and virtual appliances and server software. They make the task of collecting, correlating, and action on threat information easier for security teams.

(iv) Network security analytics. Advanced network security analytics solutions offer organisations comprehensive threat visibility into the extended network. They can simplify network segmentation by using behavioural modelling, machine learning, and global threat intelligence.

Email security software: Email gateways are the top vector for a security breach. Phishing, ransomware, business email compromise, and other inbound threats are just some examples of threats that email security software can help detect and deflect. Email security applications can also control outbound messages to help prevent the loss of sensitive data.

Internet of Things (IoT) security software: The Internet of Things (IoT) involves the interconnection through the internet of computing devices inserted in every single object, allowing them to send and receive data. Hence, if one object can prevent the internet of things from transforming the manner we live and work, it will be a breakdown in security. As the IoT expands, organisations need security software to help them understand what is touching their network, handle more complex access management tasks, secure endpoint access, and much more.

Internet security. Sources: ***http://eprints.covenantuniversity.edu.ng***

3.3 Software security Lifecycle

A software security lifecycle involves a continuous identification, analysis and management of information security risk throughout the lifespan of information or data. The value placed on information by an organisation suggests the height it will go to prevent and protect its vulnerability to avoid its loss or unauthorised access and use. The software security architecture does harvest information security risk by way of identification, refines it by analysing the threat, thereafter, proffers solutions or information on how well to manage both the information and the system. In other words, the software security lifecycle strives to identify, analyse and manage the threat, actor, asset risk and outcome of information.

Software Security Lifecycle. www.evansonline.com

Software Security Lifecycle

Information software security is built to identify, analyse and manage data via the following elements in the

- **Threat**: This involves the actors or events
- **Actor:** Actors here represent an external or external entity to the organisation that owns the asset which may violate some security properties of an asset.
- **Asset:** This is something that is of value to the organisation such as personnel, software system and /or information in electronic or physical form.

- **Risk:** An expectation of loss expressed in terms of the likelihood that a particular threat will exploit a particular vulnerability with a (harmful) result in terms of impact on the business or mission. Impact may be expressed in terms of cost, loss of business/mission effectiveness, loss of life, etc.
- **Outcome:** This is the direct consequence or the result of going against the security property of an asset including deleting, service denial and modification (DHS 2006)

3.4 How to secure software resources

Nowadays, the global economic, social and political space is filled with information and information, they say, 'rule the world' especially in this 21st century. Then, it is one thing to create information either software or print and it is another thing all together to secure the information being created. It is disastrous for individuals, groups, organisations and governments not to protect and secure the information and allow such get into wrong hands or channels. Bird (2015) listed 10 steps to follow to achieve a secure software information as follows:

Protect your database from SQL injection: To have a secured software, it is advisable to guide against SQL injection. SQL injection is a code injection procedure used by attacker to attack data driven application where mischievous SQL statements are injected into an entry for execution.

Encode data before using it: In a way to secure your information from unauthorised access and use, you need to encrypt it by making it safe before handing it off to an external interpreter such as OS command shell or browser, or XML,

Validate input data before you use or store it: All data from external sources should be authenticated before using them no matter how authentic the source may appear. Data validation rules imply; first, you do not rely on client-side checking, you must always check your server. Second, use positive, whitelist validation rule where possible

Access control deny by default: All system functions must be checked. This is to ensure that users are authorised before gaining access to the information. Therefore, decide who needs access to which information and to which features and uphold how these rules will be enforced.

Establish identity upfront: The best ways to do this is to apply multi-faction authentication and the application of lengthy and complex User ID and Password.

Protect data and privacy: Data need to be secured at creation point to transit period and during storage via encrypting it at every stage. You should keep in mind and endeavour to avoid the

common mistakes which normally occur during information encryption which include:

i) Forgetting to encrypt data in the first place
ii) Trying to roll your own encryption algorithm
iii) Mishandling keys or other setup steps for standard encryption libraries

- **Logging and intrusion detection:** Logging strategy is vital for system troubleshooting, debugging or fixing detected issues which are critical for activity auditing. Whereas intrusion detection entails telling operating systems when system is being hacked. In addition, system forensic figures out what happened after the system is hacked. Therefore, you need a good logging and intrusion detection strategy to secure your software.

- **Do not roll your own security code:** It is advisable to take time to study, understand, use and take advantage of the security capabilities of your application framework and security libraries such as Apache Shiro, Spring security, Ruby on Rails, NET etc, which can take care of common security problems rather than rolling your own security code.

- **Handle errors and exceptions correctly:** A study by University of Toronto discovered that mistakes in error handling can lead to catastrophic system failure in a large system. These errors include leaking information that hackers can use to penetrate your system, missing or inconsistent error handling which can lead to errors going unnoticed, unpredictable behaviour or crashes.

- **Build security testing into development:**
  Security checks should be included in code reviews, and security testing needs to be automated and included in Continuous Integration and Continuous Delivery pipelines. Make sure that you have functional automated unit and integration test coverage for security features and controls (like authentication, access control, and auditing) and critical business features: code that handles secrets, and admin functions. This must include both positive and negative tests (Bird, 2015).

3.5 Possible Solutions to software Security Challenges

The contemporary method of securing information involves enforcing access control through the following measures:

i. **Validation of input to an application:** The validation of data input is a set of controls that an application should carry out on the lexical and syntactic aspects, type checking,

integrity, and origin of data. The lack of these controls has become a major problem for software because interfaces exposed to the Internet could be easily exploited by malicious users (Brinhosa et al. 2013).

ii. **Installation of antivirus:** Viruses and malwares can cripple your computer and destroy your files. Antivirus programs are designed to find and intercept viruses before they do any harm. An antivirus program is essential on a Windows PC and can be very useful for Mac and Linux users as well. Check out this guide for whichever operating system you use (Martinez 2021).

iii. **The use of firewall to a local area network:** The use of firewall to a local network involves the installation in a compulsory passage point between the network to be protected (internal and non-secure network external). It is a different set of hardware and software component that controls the traffic inside/outside according to established security rules. In essence, it is typically built as a barrier between a trusted and untrusted network

iv. **Employing Transport Layer Security (TLS):** This system is designed to support privacy and data security for communication over the internet by encrypting communication between web application as well as server (web browser loading a website).

Other ways according to APIEST (2019) include:

v. **Authentication mechanism and authorization**. This process includes a well-designed system that prevents the user from changing identity without re-authentication, multifactor authentication, a security control mechanism, resource authorization, file and database permissions, etc., an examination that protects any software from problems associated with authentication.

vi. **Data validation: In the development life cycle**, the Brain Station 23 always focuses on the data validation process, which includes centralized validation mechanisms, converting data into canonical form, using common libraries of validation primitives, and implementing language-level types to collect data assumptions. etc.

vii. **Cryptography:** Cryptography is one of the most important tools for building secure systems. With proper use of cryptography, the Brain Station 23 ensures data privacy, protects data from unauthorized changes, and authenticates

the source of the data. Cryptography can also provide many other security goals.

viii. **Identifying and processing confidential data**. One of the most important tasks that the Brain Station 23 developers perform is to identify confidential data and determine how to protect it properly. Data sensitivity depends on many factors, including regulation, company policy, construction obligations and user expectations, etc. Technical data sensitivity includes access control mechanisms (including file protection mechanisms, memory protection mechanisms and database protection mechanisms), cryptography to preserve confidentiality or integrity of data, backups and backups to maintain data availability, etc.

ix. **Analysis of the impact on the security of the integration of external components:** when integrating any third-party applications into any software, there is a significant risk to attract certain threats that accompany third-party integration. Brain Station 23 analyses the errors from third-party applications that may be disguised as software errors, access problems between third-party applications and specific software, incompatibility between third-party applications and software interfaces, etc., to ensure that any external integration works as expected. and does not affect existing software functionality.

x. **Audit trail:** This process records security-related chronological events that are very important in terms of security and process improvement. Brain Station 23 provides compliance programs for specific industry needs, such as CSA for managing the Cloud Security Alliance, PCI for payment card standards, FIPS for state security standards, FISMA for federal information security management, HIPAA for protected medical information, etc.

Security challenges: Source http://eprints.covenantuniversity.edu.ng

3.6 Process for software security

Software security is vital to all that create, store and use information for personal, commercial purposes and even in doing government business. Thus, the process of software security involves the development, application and use of a laid down practice, and procedure to secure vital information from being accessed, intercepted and used by unauthorized users. Software security is an integral part of the software development lifecycle. Spacey (2011) highlighted a simple process for software security as follows:

- **Constraints:** Security needs to take account of constraints such as

  Budget: A good process ought to take into consideration the budget which entails an estimation of revenues and expenses involved in the software security

  Time: This has to do with period, phase and interval as it concerns the software security

  ***Target architecture*:** This involves a holistic model of the applications required to fulfil software security need and support target processes

- **Tools:** A Security testing tools can systematize responsibilities such as vulnerability and penetration testing. In other words, security tools can assist in establishing security necessities, build excellent gates, accomplish threat assessment, model threats and categorize shared and branded vulnerability to security threats.

- **Techniques:** Security design patterns which constitute the techniques in software security are critical to the process of building secure software

- **Common vulnerabilities:** When designing, developing and testing software security, it is important to consider shared security vulnerabilities.

- **Known vulnerabilities:** The known vulnerabilities in mechanisms, APls, server and algorithms need to be investigated in the process of software security development and application
- **Common threats:** At each stage of the Software developing lifecycle, common threats to software SQL injection and cross-site scripting needs to be considered:
- **Security architecture and design:** The development of a secured software starts with securing the security architecture and design**.** Faulty design proves more serious vulnerability than software bugs
- **Security review:** This requires series of both formal and informal code reviews, because software security designers can repeatedly identify its weaknesses in the code that are difficult to discover in testing
- **Security testing:** It is possible to automate many black box security tests such as vulnerability scans and penetration tests (Spacey, 2011).

4.0 CONCLUSION

Systems users or organisations operating without information security software or using an outdated security software stand the risk of exposing the system to a wide range of threat such as viruses, hackers, malware and spyware. Therefore, the software security and authentication protocol are intended to secure and protect networks, laptops, servers as well as mobile devices from threats, intrusions, viruses and unauthorized persons. It is also designed to proffer defence to computer users, data, companies' sensitive information and systems from a wide range of threats...

5.0 SUMMARY

In this unit, we discussed software security and authentication protocol, and highlighted the meaning of software security. Also discussed in this unit include:

- Ways to software security practice
- Forms of software security programs
- Possible solution to information security challenges

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

i. List and explain types of authentication protocol
ii. Forms of security software programs
iii. Highlight and explain possible solution to information security challenges

7.0 REFERENCES AND FURTHER READING

APIBEST (2019) Importance of software security. Retrieved from https://apibest.com (7th November 2020)

Bertino, E., Martino, L., Paci, F., & Squicciarini, A. (2009) *Security for web services and service-oriented architectures.* New York: Springer Verlag, 2009.

Bird, J. (2015) 10 steps to secure software. Retrieved from https://dzone.com (4th February, 2021)

Brinhosa, R. B., Westphall, C. M., Westphall, C. B., Ricardo dos Santos, D., & Grezele, F (2013). A validation model of data Input for web services. Retrieved from https://daniel-rs.github.io **(**7th November 2021)

Department of Homeland Security(DHS) (2006) security in the software lifecycle making software development processes— and software produced by them—more secure draft version 1.2 - Retrieved from https://resources.sei.cmu.edu (11th March 2021)

ISSA (2011) Information Security for South Africa. Retrieved from https://digifors.cs.up.ac.za/issa/2011/index.htm (3rd March 2921)

Martinez, G. (2021) How to install antivirus. Retrieved from https://www.wikihow.com (4th May 2021)

Sadiku, M. N. O., Shadare, A. E., Koay, S. & Musa, S. M. (2016) Challenges of information system. Retrieved from https://qsstudy.com (5th May 2021)

Technopedia (2012). New word suggestion. Retrieved from https://www.collinsdictionary.com

UNIT 5: PRINCIPLES AND NETWORK SECURITY FOR PRESERVING, CONSERVING AND SECURIING LIBRARY ITEMS

CONTENTS

1.0 INTRODUCTION

This unit brings you to the principles and network security for preserving, conserving and security library items. We will also discuss the different forms of the principle involved in the information security in general terms which is also applicable in library services delivery.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

At the end of this unit, you are expected to explain the meaning of the basic concepts of the principles of security as well as the forms of information security principles

3.0 MAIN CONTENT

3.1 Principles of Information Security

The security goals/principles in information are Confidentiality, Integrity, and Availability.

Information security. Sources: https://www.securitymagazine.com/articles/95681

These three features are known as the CIA triad: C for Confidentiality, I for Integrity, and A for Availability. Fruhlinger (2020) elaborates on these principles according to CIA triad thus:

> **Integrity:** This deals with the question of reliability of the carrier and custodian of the information**.** It is an act of maintaining data in its correct form and avoiding its being wrongly altered, either by accident or maliciously. Many of the techniques that ensure confidentiality will also protect data integrity—after all, a hacker can't change data they can't access—but there are other tools that help provide a defence of integrity in depth: checksums can help you verify data integrity.
> For instance, and version control software and frequent backups can help you restore data to a correct state if need be. Integrity also covers the concept of non-repudiation: you must be able to *prove* that you've maintained the integrity of your data, especially in legal contexts. Integrity is said to be violated when a message is actively altered in transit. In library service delivery, integrity may tend towards providing reliable structure through which the safety of library information resources could be guaranteed
>
> **Availability:** This is the process of making information or data obtainable and accessible for the rightful persons. It is the mirror image of confidentiality: while you need to make sure that your data can't be accessed by unauthorized users, you also need to ensure that it can be accessed by those who have the proper permissions. Ensuring data availability means matching network and computing resources to the volume of data access you expect and implementing a good backup policy for disaster recovery purposes. By implication, library service delivery includes providing available access to the library material resources for clients.
>
> **Confidentiality:** This is the act of concealing information from unauthorised persons. It is perhaps the element of the triad that most immediately comes to mind when you think of information security. Data is confidential when only those people who are authorized to access it can do so; to ensure confidentiality, you need to be able to identify who is trying to access data and block attempts by those without authorization. Passwords, encryption, authentication, and defence against penetration attacks are all techniques designed to ensure confidentiality. The part of library information security enables the library to screen and verify information before its dissemination. It is also to ensure the confidentiality of the library users.

Ideally and in practice, sensitive library data should always be kept confidential, reliable and available in its correct state. Librarians need

to make the choice of information security principles to be emphasized, and the one that is required in assessing the data. For instance, if you're storing sensitive medical information, you'll focus on confidentiality, whereas a financial institution might emphasize data integrity to ensure that nobody's bank account is credited or debited incorrectly.

4.0 CONCLUSION

The principles and network security for preserving, conserving and security library items involves securing information resources through the application of triad of confidentiality, availability and integrity (CIA) principles in the provision of library services delivery.

5.0 SUMMARY

The principles of information security includes application of Integrity which has to do with the question of reliability of the carrier and custodian of the information; availability as a process of making information or data obtainable and accessible for the rightful persons and confidentiality**,** that has to do with the act of concealing information from unauthorised persons.

6.0 TUTOR-MARKED ASSIGNMENT

List and explain the three major principles of information security

7.0 REFENCES/FURTHER READING

Fruhlinger, J. (2020). What is information security? Definition, principles, and jobs. Retrieved from https://www.csoonline.com/article/3513899/.html (4th June 2021)

MODULE 4: OPERATIONAL AND ORGANISATIONAL SECURITY

INTRODUCTION:

Our emphasis in this module, is the operational and organisational security, software security and authenticated protocols as well as the challenges of the preservation and security of library and information systems and resources in Nigeria. It will give you the opportunity to identify and analyse the various ways of achieving and maintaining excellent security operations within the library and for the library materials.

Unit 1 Operational and organisational information security

Unit 2 Data integrity, provenance and digital signatures.

Unit 3 Security authentication protocols

Unit 4 Data Management

Unit 5 Challenges of preservation and security of library and information systems and resources in Nigeria

UNIT 1 OPERATIONAL AND ORGANISATIONAL INFORMATION SECURITY

CONTENTS

1.0 INTRODUCTION

In this unit, you will be introduced to the concept of operational security on one hand and organisational security on the other. Also, we will examine the different approaches, guidelines, standard, policies and procedures as well as steps to achieving operational and organisational security.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

At the end of this unit, you should be able to:

i. define and explain the operational and organisational security process;
ii. analyse the approaches to organisational security,
iii. discuss the steps to achieve effective organisational security.
iv. identify the importance of operational and organisational security as well as what constitute the barriers to organisational security

3.0 MAIN CONTENT

In general terms, organisational security involves the application of policies and procedures which guide the security operator's interaction with information and information processing systems to secure a successful security program which are in line with the organisational set goals and objectives.

3.1 Organisational Security

Organisational security network: *https://encrypted-tbn0.gstatic.com*

What is Organisational Security?

Dunn (2015) defines organisational security as a sustained appropriate level of security in team communication and information management

practices. He further stated that organisational security has much to do with the social and political decision-making of an organisation. Security isn't about the perfect technical fix; it's about working with all members of the team to make sure they understand the issues and the value of protecting information. Supporting awareness raising activities to encourage individual thinking about security (in addition to how-to's, instructions, and policies) is key to supporting longer term growth and more organic adaptation to new threats.

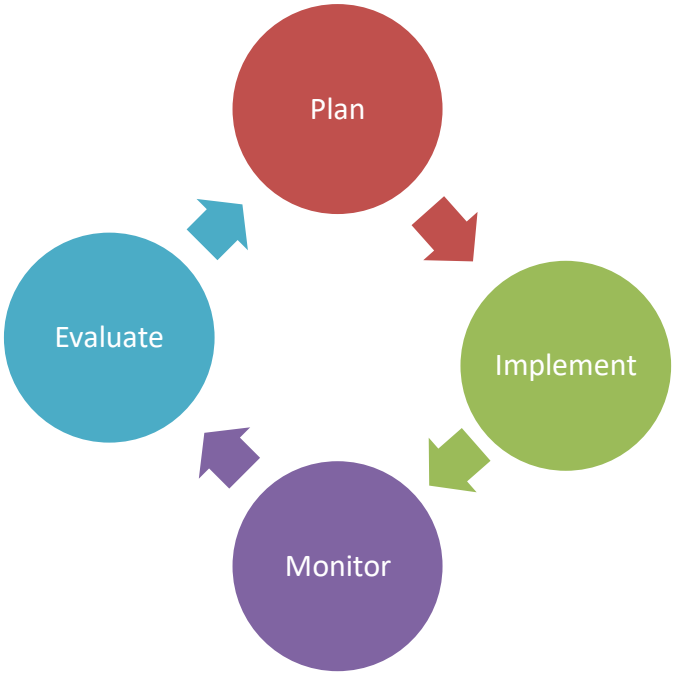
Also, Mosso (2020) defines it as a group with common operational and substantive aims, with shared and agreed practices towards protection from threat, integrity of systems, and the safety and wellbeing of individuals. In addition, Mosso (2020) maintained that organisational security is the organisational control of data and how it is used (and by whom) - without any loss of control.

To have a robust and well-defined organisational security framework, it is ideal to focus on both information technology and security which serve as basic requirements for the success of the organisation or institution. Mostly, organisational security can be seen as a barricade. It is the only way to enhance the protection of an organisation's data from threat in order to avoid information compromise. Obviously, prevention technology is not enough to protect the organisational data from compromise. More and detailed approaches such as prevention, detection and response technologies should be put in place in order to have the organisational data ultimately secured..

3.2 Approaches to Organisational Security

Organisations ought to formulate and implement essential approaches that provide organisational security details to the information security operators within the organisation. These approaches include:

1. **Policy:** This is a high-level or management statement of plan that embraces the general organisational security goals and acceptable procedures toward achieving it. Policies are made by the management when laying out the organisation's position on certain issues. Every organisational security policy must operate like a lifecycle.
   Policy lifecycle: For the fact that security network itself changes constantly, the approaches to it also change and revolves on a cycle to retain its relevance.



Organisational security life circle: **(Self constructed)**

Plan: The proposal and strategies to be adopted. It could be adjusted to suit any security prevailing situation in an organisation
Implement: To give a practical effect and ensure actual fulfilment of the plan
Monitor: Keeping track or watch over the implementation process
Evaluate: Appraising theeffectiveness of the whole organisational security plan/policy

2. **Procedure:** This approach involves the step-by-step techniques, processes or instructions on how to implement policies in the organisational security. Procedures describe precisely how staff are expected to act in each condition or to complete a definite task, especially as it concerns information security.
3. **Standard**: Standards are accepted specification that provide specific details on how a policy is to be enforced. They appear as mandatory elements regarding the implementation of a policy. Some standards are externally driven. For instance, such as banking/financial regulations or laws, whereas other standards may be set by the organisation to meet its own security goal.
4. **Guideline:** This acts as recommendations which relate to the already formulated and implemented policies. It is a perimeter to the organisational security policy. Therefore, it may not be a mandatory step.

The policies, procedures, standards, and guidelines should be included in living documents that are periodically evaluated and changed as necessary. The continuous monitoring of the network and periodic review of the related documents are part of the process that constitute the operational model. When applied to policies, this process results in what is known as the policy lifecycle. This operational process and policy lifecycle roughly consist of four steps in relation to the security policies and solution.

3.2 Steps to effective organisational security

Bandos (2018), listed 9 steps to achieve effective organisational security and these include:

- **Take a risk-based approach.** A risk-based approach especially with employees is considered essential approach to organisational security. No matter the cadre or position of the employee, determining where the most risk resides should always be one of the first things done in an organisation.
- **Provide incentives for good behaviour:** Another important step in developing a security awareness program, can often feel like an effort in futility. Simply communicating what's expected of an employee from a security perspective or foisting a campaign on users isn't always effective. Organisations commonly deploy one-size-fits-all approaches that rarely succeed in altering employee behaviour over time. These types of campaigns don't need to go away — they likely never will — but they should give incentives to participants and reward good behaviour. Users shouldn't get shamed for accidentally clicking on a phishing link. Instead, they should feel like they play a pivotal role in strengthening the organisational control of a company.
- **Incorporate technology:** That doesn't mean it's not good to take some decision-making work away from employees. If you're relying on an employee to do the right thing all the time, you're going to fail eventually. Some see security as a burden on a user, but it doesn't have to be like that. Technology, the more transparent and seamless the better, can help take the guesswork out of situations. Having a well-balanced security strategy paired with those technologies should be the goal of every enterprise.
- **Stop and think:** Employees should learn to adopt a stop-and-think mind-set. If an employee receives a phishing email, she should pause and ask herself "Is this something I should be doing?" before clicking through. The routine should become habitual, almost instinctive over time. An employee can be the last link in the security chain, but if that person clicks on something malicious, that chain is broken and has opened the enterprise to a possible breach

- **Assign a leader:** Depending on the size of a business, it could prove beneficial to assign a security leader to each segment across the organisation. The leader can confer with other leaders and collaborate on pressing security issues. Every time users have a question — about a potentially malicious link or any other issue — they should be able to ask someone about it quickly. Without a leader, someone dedicated to answering questions, users could be tempted to click on that link, something that could lead to bad decision-making behaviour down the line.
- **Get other departments involved:** Organisational security doesn't need to be confined solely to the IT department. It's important to leverage resources you have internally. The marketing department can even play a role. One of the main goals across an organisation should be to build a security brand within the company. Tapping into the marketing department, a group of individuals that know how to position itself, what reaches people, and how to measure it, can be enormously helpful.
- **Set up policies:** Some of these suggestions may sound esoteric, but at the end of the day, employees still need to answer to something. That's why policies should set up and enacted. If you don't hold employees accountable for their actions — what sites users can browse to, what they're allowed to do on their machines, etc. — all of this will be for naught.
- **Refer to published frameworks:** When it comes to published IT management frameworks, there are some great guides already on the books. The National Institute of Standards and Technology (NIST) has some guidance. Control Objectives for Information and Related Technologies, or COBIT, an auditing/compliance framework, can also help outline governance and management practices. Not everything may make sense for your company or your organisation but developing your own policies on the fly is never a great idea. Align with industry best practices; after all, they're considered best practices for a reason.
- **Take your time:** There's no reason to rush. This isn't something that happens overnight. It can sometimes take years for a company to deploy a successful security awareness campaign. Corporations too often take a tactical approach while rolling out campaigns when they should be more realistic. Take a strategic approach and plan over the course of several years, not months' (Bandos, 2018).

3.4 Operational Security

The need for Operational security '*OPSEC"* cannot be exaggerated especially in keeping an information away from internal and external threat.

Security Operational Centre: en.wikipedia.org

What is Operational Security?

CDSE (2020), defines Operations Security (OPSEC) as the process by which we protect critical information whether it is classified or unclassified that can be used against us. It focuses on preventing our adversaries' access to information and actions that may compromise an operation. OPSEC challenges us to look at ourselves through the eyes of an adversary and deny the adversary the ability to act (CDSE, 2020).

Also, Zhang (2020) states that Operational security (OPSEC), also known as procedural security, is a risk management process that encourages managers to view operations from the perspective of an adversary to protect sensitive information from falling into the wrong hands. Though originally used by the military, OPSEC is becoming popular in the private sector as well. Things that fall under the OPSEC umbrella include monitoring behaviours and habits on social media sites as well as discouraging employees from sharing login credentials via email or text message (Zhang 2020)

Technopedia (2021) defines Operations security (OPSEC) as a process that involves the identification and protection of generally unclassified critical information or processes that can be used by a competitor or adversary to gain real information when pieced together. Although the information sought under OPSEC isn't classified, it could give a competitor or other adversary an advantage. OPSEC focuses on the identification and protection of information that could give enemies clues or capabilities to put one at a disadvantage

According to online Technology dictionary, OPSEC is a strategy used in risk management that enables a manager to view operations or projects from the perspective of competitors or enemies. The key concept of this approach is to look at one’s own activities from the outside and try to piece together readily observable or obtainable information.

It is worth noting that organisational and operational information security focussed on the reports and analysis and protections of organisation's information system from unauthorised access and use.

Operational Security (OPSEC) is an analytical process that classifies information assets and determines the controls to protect these assets. In fact, it identifies friendly actions that could be useful for a potential attacker to reveal critical information or sensitive data. Operational Security is popular among cybersecurity risk management, data protection, and information security professionals (Mahmood, 2020)

Organisational security involves the control of information, its usage to avoid loss or unauthorised access, whereas operational security involves an expertise risk management process to protect sensitive information from entering wrong hands. In other words, organisational and operational security encompass the interaction between the information system, its operators and how it works to achieve the organisation's goal.

Security operational centre ***www.exabeam.com***

3.5 The Five Steps of Operational Security

The operational security can be categorized into five steps (Zhang, 2020, Mahmood, 2020):

Identify your sensitive data: including your product research, intellectual property, financial statements,

customer, and employee information. This will be the data you will need to focus your resources on protecting.

Identify possible threats: For each category of information that you deem sensitive, you should identify what kinds of threats are present. While you should be wary of third parties trying to steal your information, you should also watch out for insider threats, such as negligent employees and disgruntled workers.

Analyse security holes and other vulnerabilities: Assess your current safeguards and determine what, if any, loopholes or weaknesses exist that may be exploited to gain access to your sensitive data (Zhang, 2020)

Assess Risk Factors: Create a Security Risk Assessment checklist for all your assets. Appraise the level of risk associated with each vulnerability. Therefore, rank your loopholes using the following factors.

- The likelihood of an attack happening
- The extent of damage that you would suffer
- The amount of work and time you need to recover

Understand that the more likely and damaging an attack is, the more you should prioritize mitigating the associated risk.

Apply Countermeasures: The last and the most critical step of OPSEC is to get countermeasures in place. Create and implement a plan to eliminate threat and mitigate risk. In addition, include updating your hardware, creating new policies, or training employees on new security patrol services. Countermeasures should be clear and simple. In short, employees should be able to implement the measures without any additional training (Mahmood, 2020).

3.6 Importance of Operational Security

1. It helps organisations safeguard their most sensitive data and prevent it from getting into the wrong hands.
2. It offers a different manner of approaching cybersecurity and data security by encouraging IT and security teams to look at their systems and processes from the perspective of potential attackers.
3. It also helps stop the inadvertent leak or exposure of sensitive data and improves organisations' security defences.

4.0 CONCLUSION

In a general term, the organisational and operational security remains one of the most important aspects of the information security both in the

library and other organisations. This is to carefully checkmate and guide data from entering unauthorised persons.

5.0 SUMMARY

Organisational and operational security are imperative in organisational efficiency. Therefore, the approaches to organisational security such as policies, procedures, standards and guidelines should be taken for topmost security in operations and the general functioning of the institution.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. List and explain the steps involve in operational security?
2. Explain the approaches to organisational security?
3. Highlight and explain the lifecycle in policy approach to organisational security?

7.0 REFERENCES AND FURTHER READING

Bados, T. (2018) 9 steps to more effective organisational security. Retrieved from https://www.mhprofessionalresources.com/sites/principlessecurity4e/download s/sample.pd (20th December, 2021)

Centre for Development of Security Excellence (2011). Operational security Retrieved from https://www.cdse.edu/index.html.com. (20th December 2020)

Computer Science Research centre CSRC (2015) security concept of operations

Retrieved from https://www.agilesecurityusa.com (3rd February 2021)

Mohmood, A (2020) Five-step operational security to protect your business

Mosso, P (2020) organisational security definition https://orgsec.community/display/OS/Organisational+security+definitions

O'Reilly Media (2021) Organisational and operational. Retrieved from

https://www.oreilly.com/online- learning/individuals.html (5th May 2021)

Zhang, E. (2020). What is operational security? The five-step process, best practices, and more. Retrieved from https://www.digitalguardian.com (4th April 2021)

UNIT 2: DATA INTEGRITY, PROVENANCE AND DIGITAL SIGNATURES,

CONTENTS

1.0 INTRODUCTION

Data integrity, provenance, signatures, management and risk assessment are issues of great importance to libraries and library operations. Data integrity entails reliability of data in terms of consistency and accuracy. Data provenance can be referred to as the custody, ownership and origin of data, while data signature has to do with the structure of mathematical scheme for verifying the authenticity of digital messages.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

Our discussion in this unit focuses on data integrity, provenance, signatures, management, and risk assessment. Therefore, at the end of the unit, you should be able to:

i. identify the essential factors in data provenance, data signature;
ii. explain the types and the functions of data integrity and ways of minimising data integrity risk

3.0 MAIN CONTENT

3.1 Data Integrity

The term 'data integrity' is wide in scope and may have broadly different meanings depending on the context one may use or apply it. Even under the same umbrella of computing, the meaning of data integrity may differ. According to Pederson (2017) data integrity is a complete, consistent, and accurate data to assure patient safety and product quality. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a 'true copy', and accurate (ALCOA). Data integrity should be maintained throughout the data life cycle, including, but not limited to data creation, processing, archiving and disposition after record's retention period. Data integrity should apply to all documents irrespective of its dynamic or static nature (Pederson, 2017).

Telan (2021), defines data integrity as the overall accuracy, completeness and consistency of data. It may also be referred to as the safety of data regarding regulatory processes. Data integrity is maintained through a collection of processes, standards and rules implemented during the design stage. Information stored in database will remain complete, accurate and reliable despite the length of storage and or the frequency of accessing it provided the data integrity is secured. Also, data integrity ensures the safety of data from outside interference.

Also, Ian (2016), defines data integrity as the accuracy and consistency of data. Ian (2016) maintains that when creating database, attention should be given to data integrity and how to maintain it. A good database will enforce data integrity whenever possible. Brook (2020) writes that data integrity refers to the accuracy and consistency (validity) of data over its lifecycle. According to him, compromised data is of little use. Therefore, to maintain data integrity should be the core focus of software security solution.

Data integrity which can also be referred to as data reliability which entails the maintenance, accuracy, consistency of data throughout its lifecycle. It is a critical aspect in the designing, implementing and use of any system that stores, processes or retrieves data. It is used to ensure that data is not corrupted, and the quality of a data is maintained. As such, data integrity technique ensures data is recorded exactly as intended and the same upon its later retrieval. In other words, it ensures that the originality is maintained.

Data integrity. afteracademy.com

3.1.1 Types of data integrity

Data integrity is categorised into the following types thus:

1. **Domain integrity**: This is concerned with the validity of entries for a specified column. The selection of suitable data type for a column remains the first phase in keeping domain integrity. Further phases could include, setting up appropriate constraints and rules to define the data format and/or restricting the range of possible values.
2. **Referential integrity**: This type of integrity is concerned with relationships. When two or more tables have a relationship, we must ensure that the foreign key value always matches the primary key value. We don't want to have a situation where a foreign key value has no matching primary key value in the primary table. This would result in an orphaned record. Referential integrity prevents users from: adding records to a related table if there is no associated record in the primary table. Changing values in a primary table that results in orphaned records in a related table. Deleting records from a primary table if there are matching related records.

3. **Entity integrity:** In database world, no two rows can contain the same unique identifier. Each row is unique within its table.
4. **User-Defined Integrity:** This type of integrity permits the user to apply business rules to the database that are not covered by any of the other three data integrity types.

3.1.2 Factors affecting data integrity

Several factors often affect the integrity of the data stored in the database and these include:

1. **Human error:** This occurs when an information is entered incorrectly, duplicated, deleted, or not following the appropriate protocol. In addition, it is when individuals make mistakes while implementing the procedures meant to safeguard information and this puts data integrity in danger.
2. **Transfer error:** When transfer error occurs and being unable to transfer data from one location in a database to another. Also, when a piece of data is not in the source table in relational table but present in the destination table.
3. **Bugs and viruses:** Different viruses, malwares, spywares are software that can attack a computer and steal, alter, or delete data.
4. **Compromised hardware:** This can limit or eliminate the access and use of data as well as render data incomplete or incorrect. This occurs when a server or computer crashes which may lead to its malfunctioning.

3.1.3 Ways to minimize risk to data integrity

The factors affecting data integrity can be minimised or eliminated through applying any of the following:

1. Validate your data to ensure it is correct both when you gathered it and when it is being used.
2. Always have a back-up.
3. Limit access to data as well as change permission in order to restrict changes to information by an authorised party.
4. Conduct regular internal software and hardware audit.
5. Use an error detection software.
6. Use logs to keep track to know when data is added, altered or deleted from your system.

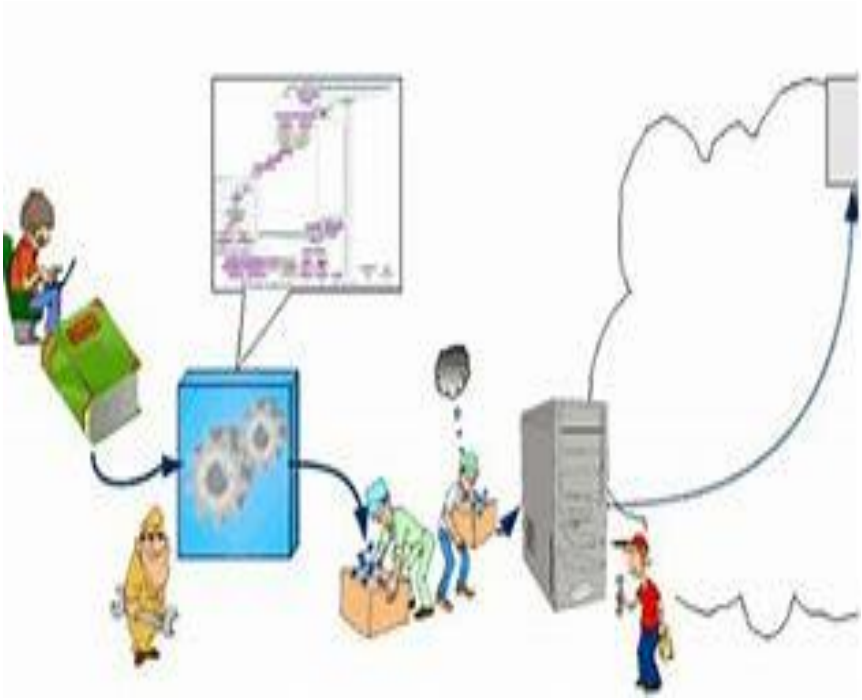
3.2 Data Provenance

Data provenance is the records of the origin of pieces of data, the processes and the methodology used in its production. The word provenance originated from French word '*provenir'* meaning 'to come from' which can also be interpreted to mean 'pedigree' or 'lineage'. According to Moreau (2015), in the world of art, the notion of provenance is well understood. When a piece of art is sold in an auction, it normally goes together with a paper trial detailing the chain of ownership of the artefact from its creation by the artist to the auction. This document is referred to as the provenance of the artefact.

In science, according to Yuan and Chen (2013), data provenance is a kind of important metadata in which the dependencies among application data

sets are recorded. The dependency depicts the generation relationship among the data sets. For scientific applications, data provenance is especially important because after the execution, some application data sets may be deleted, but sometimes the users must regenerate them for either reuse or reanalysis. Data provenance records the information on how the data sets were generated, ……on the trade-off between computation and storage.

Data provenance provides the origin, custody, lineage and ownership of research data. It is used to trace the beginning of a data. For instance, dataset are used and or reformulated and even reworked to create a new data. But data provenance helps to trace the origin of the newly created data to its original dataset. Data provenance ensures that a creator of the data is held accountable for his/her work. It also provides a chain of ownership where data can be traced or tracked.



Data provenance. Source: www.ontotext.com

Ordinarily, data provenance should record and describe in what manner agents, entities and activities have influenced a piece of data which helps in making trust judgement about the data. For instance, you know whether to trust a data if the history or origin is known for the fact that data you can easily track down inaccuracies, errors flaws, even fraud and to make a better data analysis.

3.2.1 Benefits of Data Provenance

In our present-day information/data saturated word, data provenance can generate widespread benefits which include:

1. **Secures system:** A data provenance can be a system lifesaving in one of the most terrifying examples of a breach in data security. Particularly, data provenance would make it immediately noticeable when a new code enters a system. Also, the inclusion of data provenance in the systems cyber-security strategy ensure rejection of poisoned data and alleviate 'weaponised' data.
2. **Creates new lines of business:** Technologies and information explosion has brought about Internet of Things (IoT) which has created flood of data. Thus, data provenance supports organisations to quickly identify odd or fake data, by creating faster ways of cleaning data and creating actionable business models. In addition, provenance allows new business models that compensate the rightful owner of data for sharing. In other words, people who share their personal data with the company ought to be compensated for doing so.
3. **Restores credibility:** Data credibility and trust have proven problematic particularly in scientific research, but the increase in compliance regulation seems to be providing corresponding positive response to the problems. Interestingly, data provenance restores credibility by allowing users of information to easily track data to its origin. It also enhances certification of the authenticity of the data because data is more easily traceable and searchable.
4. **Artificial Intelligent (AI):** Artificial intelligence can only work when a quality data set is ingested. In essence, data provenance ensures the traceability of the quality, relevance and complete data which is used by the AI. Artificial intelligence fails when a poor or less quality data is fed on it.
5. **Maximise metadata:** Quality metadata is essential for reusing and repurposing data sets, yet its full value is rarely realized. Data teams spend large amounts of time cleaning and organizing data. Once used, that same data is often stuffed and forgotten in online storage. Data provenance, by tracking the history of every piece of data, essentially automates part of the metadata creation process, cutting times spent cleaning and organizing data. Lineages also make it easier to access metadata, reuse old data, and combine data sets in novel ways. Machine learning applications, for example, can be trained on datasets that are pre-verified to be clean and quality assured, making model building faster and easier for data scientists (Platz 2021).

3.3 Digital Signatures

The importance attached to data has made it imperative for individuals, organisations and even the government to seek for ways to secure it from unauthorised access, alteration and use right from the data's creation, storage, location and while on transit. Data or digital signature has

become the technique that authenticates data between the senders and the recipients. According to Tanwar (2021), digital signature is a technique that guarantees that the contents of a message have not been altered in transit. This indicates that once a user digitally signs an email, it adds a simplex hash value (encryption) to the message content with the help of public and private key combination.

Digital signature. Source www.hrtechnologist.com

Furthermore, it is a calculated arrangement which verifies the authenticity of a digital message. When a recipient wants to confirm and be sure that a digital message was indeed sent by the sender, and there is no modification or alteration on the transit, then the sender needs to digitally sign the message. The digital signature strategy creates a signature which the server's public key can encrypt. Therefore, on receiving the message, the recipient can scan it. Also, with the assistance of the public key, the recipient can validate the sender and the integrity of the content of the message. Thus, on arrival of the message, if the digital signature does not match the origin of the public key within the digital certificate, then the recipient will become aware that the message has been modified or altered.

3.3.1 Keys in digital signature (Cryptography)

Digital signature is performed via public key cryptography's two mutually authenticating cryptographic key. This key is an arrangement of numbers or digit which are randomly generated. It could be complex and unique. There are two types of keys which are used to encrypt and decrypt the digital messages, namely:

Public Key: This key is used to encrypt email messages. It converts plaintext into ciphertext. Ciphertext cannot be read by humans.

Private Key: This key converts the ciphertext into human readable format. It is used to decrypt email messages. If the messages are encrypted by public key, then the recipient can decrypt the message using a private

key. A data creator creates the digital signature using a private key to encrypt signature related data, whereas the only way to decrypt this message is using the signer's public key.

Encryption: This is the act of converting electronic data into another formula known as cipher text which cannot be easily understood by anybody but the authorised parties. This guarantees data security.

Decryption: This is the procedure of translating code to data. Normally, information/message is encrypted by the sender using different encryption algorithms and decrypted by the receiver with the help of the decryption algorithms. To ensure data security, some messages are kept secured such as username, password via the use of encryption and decryption techniques.

A digital signature helps to verify the authenticity of either digital record, message or document. A valid digital signature that satisfies the fundamentals of the sender gives the recipient strong conviction to believe that the message was created by a known source/sender. Therefore, it is authentic. It also proves the integrity of the message which shows that the message was delivered as created by the sender and was not altered while on transit. Digital signatures are commonly used for financial transaction, contract management software and software distribution as well as in other situations where it is important to detect tempering and forgery because it is a standard element of most cryptographic protocol suites.

3.3.2 Types of Digital Signatures

A digital signature has basically three types divided according to certification in classes, and these include:

1. **Class 1**: This type of digital signature gives assurance that information provided in either digital data, message or document by the owner should not conflict with the information in the organised database and any issues, risk or data compromise, should not have a major significance to the environment.
2. **Class 2:** This type of digital signature is used to confirm that the owner's information should not conflict with another recognised database. It includes the transactions that have a significant value of risk and fraud and can be issued for both personal and private individuals.
3. **Class 3:** It used by both individuals and organisations when and where the level of failure of security service is high. It gives high degree security for documents, records or digital data especially when the threats to data are at high risk and the level of fraud is also high.

Digital signature https://www.hrtechnologist.com

3.3.3: Importance of digital signature

Tanwar (2021) listed the following as the importance of digital signatures thus:

i. It provides the highest level of security and acceptance accessible.
ii. It associates the signer firmly with a document during recorded dealings.
iii. It serves as electronic 'fingerprint' among the structure of a coded message for email file.
iv. Digital signatures prune the danger of duplication or alteration of the document itself.
v. It makes sure that the signatures are verified, authenticated and legit.
vi. Signers are supplied with PINs, passwords, and code which will certify and verify their identity and approve their signature.

Also, Pedamkar (2020), listed the importance of digital signatures as follows:

a) It gives the non-denial of the message.
b) It provides the message authentication particularly when the recipient validates the digital signature with help of public key that is sent by the sender as it corresponds with the private key.
c) It provides data integrity.
d) Only the owner of the data can create a sign-in for the data as unique.

e) It is necessary to exchange the encrypted message to achieve authenticity of data or message.

In a nutshell, data or digital signatures are helpful to the sender and recipient. On one side, the recipient can decline the message that does not match the algorithm's output and on the other hand, it provides a proof should there be a dispute between the parties involved.

4.0 CONCLUSION

The growth of ICT and all that are associated with it have brought about increase in the volume of data being created by individuals and organisations in their pursuit of set goals and objectives. Several measures have been developed by experts to gather, store, manage, control and secure data being produced and used. These measures aim at protecting information and preventing it from being accessed, modified and used by unauthorised persons.

5.0 SUMMARY

The importance and place of data integrity, provenance and signatures has been discussed. We examined data integrity as the reliability of data in terms of consistency and accuracy. Data provenance can be referred to as the custody, ownership and origin of data, while data signature has to do with structure of mathematical scheme for verifying the authenticity of digital message. Similarly, data management involves the act of ingesting, storing, organising and maintaining the data that are created.

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. Discuss the concept of data integrity.
   (a). List and explain the usefulness of data integrity to an organisation
2. Explain the term digital signature
   (a). Differentiate between encryption and decryption
3. What do understand by data provenance?
   (a). List and explain its benefits

7.0 REFERENCES/FURTHER READING

Brook, C. (2016). What is data integrity? definition, best practices and more. Retrieved from https://digitalguardian.com (29th June 2021)

Moreau, L. (2015). Aggregation by provenance type: a technique for summarising provenance graphs. Retrieved from https://www.academia.edu (29th June 2021)

Pedamkar, P. (2020). Digital signature type. Retrieved from https://www.educba.com (4th July 2021)

Platz, B. (2021). 5 ways data provenance can benefits your business. Retrieved from https://www.dataversity.net (5th march 2021)

Stedman, C. & Vaughan, J. (2019). What is data management and why is it important? Retrieved from https://searchdatamanagement.techtarget.com (5th march 2021)

Talend (2021). What is data integrity and its importance? Retrieved from https://www.talend.com (7th July 2021)

Tanwar, A. (2021). Digital signature in cyber-security informative. Retrieved from https://www.educba.com (6th April 2021)

What is data integrity? Retrieved from https://database.guide (7th July 2021)

Yuan, D. & Chen, J. (2013). Computation and storage in the cloud Retrieved from https://www.sciencedirect.com (3rd March 2021)

UNIT 3: SECURITY AND AUTHENTICATION PROTOCOLS

CONTENTS

1.0 INTRODUCTION

This unit exposes you to the meaning of authentication protocol and how to apply them in the root of protecting and managing information resources.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

At the end of this unit, you are expected to be able to:

i. define and explain the meaning of software security and authentic protocol
ii. identify the various types of authentic protocol
iii. recognise and explain the handshake process.

3.0 MAIN CONTENT

3. 1 Authentication Protocol

The question to ask is: do organisations require any form of authentication protocol in their operations? In this section, we are examining the need for an organisation to employ reliable and genuine procedures which culminate into protocols that help in protecting its sensitive information. By this we will attempt to explain the meaning of authentication protocol and identify the various types and their applicability.

What is Authentic Protocol?

Griffin (2021) defines authentication protocol as a computer system communication protocol which may be encrypted and designed specifically to securely transfer authenticated data between two parties.

Griffin illustrated this further by examining the process of a bank transferring money to another:

- First, completion of necessary paperwork (user verification and authentication) from the transmitting bank
- Second, secured armoured vehicle (authentication protocol)
- Third, carrying the cash in concealed packaging and unidentifiable vehicle (**encrypted data**) to the receiving bank

According to Prakash & Kumar (2018), authentication is the methodology which permits the sender and the recipient to approve one another. It can be done by offering a username and a password to identify each other against a legitimate record in the database. In other words, to check whether the combination is correct. If the user is confirmed valid then the server permits him to get to the server's assets. To this end, authenticated protocol protects the server's assets by preventing an unauthorized user to gain access to the information therein.

Nowadays, most of the libraries and other service institutions are going online. Thus, a lot of both personal and cooperate information get on the internet and it is essential to keep them secured from hackers and unauthorized users to avoid leaks. Each time we apply an authentication system, it is used to get access to a service. Thereafter, the system releases the identity in terms of username, passwords and biometric information, which can be abused (if not properly guided) by the service providers for tracking our behaviour, profiling our usage of the service or even for impersonation. Therefore, with the sharp increase of the number of services getting online treatment, it is reasonable to expect a high demand for secure and reliable authentication system.

Wikipedia described an authentication protocol as a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It permits the receiving unit to confirm the connecting unit (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax. Authentication protocol is considered the utmost important layer of protection required for protecting communication within computer networks.

3.2 Types of Authentic Protocol

Different types of authentication protocol exist for use, which provide security for sensitive information from leaking. Griffin (2012) mentioned some of them to include:

i. **Password Authentication Protocol (PAP)** It is a user authentication protocol that sends the credentials to the authentication server unencrypted as plain text. It is considered one of the simplest of all the authentication

protocols because it transmits password (data) in a plain readable text as a single readable file. Also, PAP usage increases the vulnerability of data when exchanged between user machine and servers. Furthermore, PAP is useful when the software installed in a system is not harmonious with standard secure protocol such as Challenge-Handshake Authentication Protocol (CHAP). Also, when there are a lot of vendor implementation of the CHAP within the environment creating compatibility challenges and in system recreation situation, plain text passwords are compulsory to be used during testing.

ii. **Shiva Password Authentication Protocol (SPAP):** This is a higher version/brand of PAP which offers more security. SPAP processes password via a reversible encryption system which makes them more secure than PAP's plain text authentication password. It is useful because a SPAP client system can connect to a windows 2000 server running Remote Access Service (RAS). Also, a Windows 2000 XP system connects to SPAP client.

iii. **Challenge Handshake Authenticated Protocol (CHAP):** This is an industry standard communication protocol that uses the MD5 Hashing scheme for authentication. The hashing scheme processes the information to be transmitted by scrambling it into a format that cannot be reversed into its original form. This is referred to as a one-way hashing mechanism.

The process of CHAP Authentication goes through a three-step process referred to as a handshake.

3.3 The handshake process:

(i) The requester establishes a link with the server and the server responds by sending the requester a challenge message. The requester responds with a value (processed through the MD5 one-way hashing scheme).

(ii) The server armed with a predefined calculation of the expected value (known as a challenge value or CHAP identifier) checks the value sent.

(iii) If the values match, then authentication is complete, and the communication is established. If, however, the server does not get a match on the values, the connection is terminated, and authentication fails.

CHAP however has an additional layer of security, in that the authentication is not just a one-time process as described above. For the duration of the connection the server prompts the connected party for a new challenge value at

frequent intervals and each time authentication must be successful to maintain the established connection. CHAP identifiers are therefore frequently changed throughout the duration of the connection. CHAP is useful because it is used by Point-to-Point protocol implementations to authenticate remote access clients.

iv. **Time-Based One-Time Password (TOTP)** Time-Based One-Time Password is an authentication protocol that uses an algorithm to generate what is called a temporary pass code used for authenticating access to any system. This passcode is changed every 40-60 seconds. One of the parameters incorporated into the pass code by the algorithm is the current time of the access instance. This ensures that each passcode is unique (Griffin, 2021).

Extensible Authentication Protocol (EAP): EAP is an authentication protocol which is defined in RFC 3748. It is an authentication framework that is designed to run on the data link layer where IP connectivity is not available. EAP was designed to work with Point-to-Point connections and was subsequently adapted for IEEE 802 wired networks as well as wireless LAN networks.

4.0 CONCLUSION

Encoded data are critical to the security of information being transferred between parties. In the library without encoding data there could be compromise, alteration, theft and unauthorised access. Therefore, the process of data authentication is very important. The process can be achieved using username and password to identify each other and checkmate unauthorised access.

5.0 SUMMARY

Authentication protocol is imperative in the library. It is a process which forms the basics of information security even in other organisations. Although there are different types of authentication protocols, they provide security for sensitive and valued information from leakage, hacking and alteration.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss the concept of authentic protocol and list the various type you know

7.0 REFERENCES/FURTHER READING

Bertino, E., Martino, L., Paci, F., & Squicciarini, A. (2009) *Security for Web Services and Service-Oriented Architectures.* New York: Springer Verlag, 2009.

Bird, J. (2015) 10 steps to secure software. Retrieved from https://dzone.com (4th February 2021)

Brinhosa, R. B., Westphall, C. M., Westphall, C. B., Ricardo dos Santos, D., & Grezele, F (2013). A validation model of data Input for web services. Retrieved from https://daniel-rs.github.io **(**7th November 2021)

Department of Homeland Security(DHS) (2006) security in the software lifecycle making software development processes— and software produced by them—more secure draft version 1.2 - Retrieved from https://resources.sei.cmu.edu (11th March 2021)

ISSA (2011) Information Security for South Africa. Retrieved from https://digifors.cs.up.ac.za/issa/2011/index.htm (3rd March 2921)

Johnson, M. (2020) Importance of security in software development Retrieved from https://latesthackingnews.com/2020/05/06/the-importance-of-security-in- software- development/ (4th May 2021)

Martinez. G. (2021) How to install antivirus. Retrieved from https://www.wikihow.com (4th May 2021)

Prakash, A & Kumar, U (2018) Authentication protocols and techniques: A survey

Retrieved from www.authenticationprotoccoldefinition.study.com (4th May 2021)

UNIT 4: DATA MANAGEMENT IN INFORMATION SECURITY NETWORK

CONTENTS

1.0 INTRODUCTION

In today's world, data has become one of the most significant assets to individuals and organisations. Therefore, the creation and management of data has turned out to be an important aspect of survival and success.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

At the end of this, you should be able to

i. define and explain the meaning of data management;
ii. analyse the benefits of data management,
iii. identify the challenges to data management
iv. explain the various types of data management

3.0 MAIN CONTENT

3.1 *What is Data Management?*

Data forms a great asset for individuals and organisations and as well acts like a leverage to organisational growth. Organisations would hardly survive without data. Indeed, it is easier to create data that could support individual and organisational development, but more difficult to manage the data to produce the desired result and prevent unauthorised access and use. Data management involves the act of ingesting, storing, organising and maintaining the data that are created and collected by individuals or organisations. In order to achieve effective data management in an organisation, the process must include a mixture of different functions that are jointly aimed at ensuring that the data in the system is accurate, available and accessible. Also, effective data management requires the

deployment of IT system that run the application to provide analytical data for decision-making. It ensures that data meets the need it is created for. In addition, effective data management also means backing up data with relevant policies governing its access and uses.

Data management process.
https://www.dataentryoutsourced.com/blog/data-management-best-practices

According to Talend (2021), data management refers to the professional practice of constructing and maintaining a framework for ingesting, storing, mining, and archiving data fundamentals. It is the backbone that connects all segments of the information lifecycle. On the other hand, Stedman and Vaughan (2019) define data management as the process of injecting, storing, organising and maintaining the data created and collected by an organisation. To attain management effectiveness, data management and data process must work together by complementing each other to ensure that the action taken by teams are informed by the cleanest and most current data available.

Act of data management https://www.nap.edu/read/24777/chapter/5

3.2 Types of Data Management

Experts in data management focus on specialties to determine the category. These include:

1. **Data stewardship**: It acts as a watch over data collection and movement. It also ensures that data policies, rules and practices are enforced.
2. **Master data management:** This type of data management ensures that the organisational work process and decision making is based on a single version of the true data gotten from all the organisation's sources that are reliable and constant.
3. **Data security:** This forms one of the most vital aspects of data management today. In this type of data management, security experts are tasked with the duty of encryption management that prevent unauthorised access and use of data. It also guides against such actions as accidental delete or movement of data. Data security management ensures confidentiality, privacy, and appropriateness in the access and use of data.
4. **Data quality management:** Data quality management is accountable for scrutinizing collected data for causal problems like duplicate records, inconsistent version etc. It also makes for defining, observing and improving data quality.
5. **Data warehousing:** Information has become one of the most important part of factors of production in today's world and its explosion has presented obvious challenges. In order to manage the information, data warehouse management offers and supervises the physical and cloud-based structure used to amass raw data and the indepth analyse to yield understanding usefulness. In addition, it enables access to data to support decision making, reporting and analysis.
6. **Big data management:** Data management involves the use of all-variety of different possibilities to describe gathering, analysing and usage of huge amount of digital information to increase operations. In other words, big data management specialises in intake, integrity and storage of the tide of raw data the other management teams use to improve operations, intelligence and security.
7. **Data governance:** This type of data management sets the law for the nation states of information. Its framework serves as a constitution that plainly outlines policies for the use and protection of institution's data. Data governance oversees the network of data stewards, quality management experts, security teams, and other people and data management processes in pursuit of a governance policy that serves as a master data management approach It deals

with designing, supervision and regulation over data management and use (Stedman & Vaughan, 2019).

8. **Data Architecture Management:** This serves as an essential part of the original architecture
9. **Data Development:** This type of data management involves the designing, analysis, building, testing, arrangement and maintenance of data.
10. **Database Operations Management:** This is data management that supports organised physical data assets.
11. **Reference and Master Data Management**: It involves managing versions and replicas of data.
12. **Document and Content Management**: It encompasses storing, protecting, indexing, and enabling access to data found in unstructured sources (electronic files and physical records).
13. **Meta Data Management**: It engages in integrating, controlling and delivering meta data

Data management: www.oceangliders.org

Peculiarity of the need of any institution may require them to use any or combination of all the approaches to build a solution that adapt their security and environmental problems.

3.3 Benefits of Data Management

Data management processes and procedures are very beneficial to the institutions. Excellent data management provides the following benefits:

- It helps to improve operational effectiveness
- It enables better decision making
- Improves agility and performance
- It helps organisations to avoid data breaches such as privacy issues and regulatory compliance problem

3.4 Challenges of Data Management

Notwithstanding the numerous benefits of data management, there are challenges associated with data management practices especially as the ever-growing, developing setting of ICT is constantly changing:

The amount of data can be overwhelming: Information explosion has created exceedingly huge volume of data which has proven difficult to manage.

Many organisations silo data: Different units, departments and teams in organisations work with data. Challenges arise when all are centrally controlled and managed.

The journey from unstructured to structured: Most data that pour into the organisational database are unstructured, before it can be used in decision making. It must be structured in a way of organising, cleaning or duplicating and these process pose a challenge to data management because can it be abrupt or rushed alone the line.

Managing the culture in essential data: Inability to identify the challenge of knowing the art of the 'how' and 'why' to access, use and control data and the potential pitfalls if data is mismanaged can become a major issue.

4.0 CONCLUSION

The world today has witnessed information explosion caused by globalisation and technological breakthrough. Consequently, there is the need to create effective system to control the large volume of information being created. The aim of data management is therefore to inject, organise, store, control and maintain data collected or created by individuals or organisations.

5.0 SUMMARY

In this unit, we have discussed the meaning of data and data management, the types of data management, benefits of data management, as well as the challenges of data management. It is obvious that effective data management requires the deployment of an IT system that runs the application to provide analytical data for decision-making and ensures that the data meets the needs it is created for.

6.0 TUTOR MARKED ASSIGNMENT (TMA)

1. Define data management
2 Mention and explain the types of data management you know

7.0 REFERNCES/FURTHER READING

Stedman, C. & Vaughan, J. (2019). What is data management and why is it important? Retrieved from https://searchdatamanagement.techtarget.com (5th march 2021)

Talend (2021). What is data integrity and its importance? Retrieved from https://www.talend.com (7th July 2021)

Teland (2021) What is data management. Retrieved from https://www.teland.com

What is data integrity? Retrieved from https://database.guide (7th July 2021)

UNIT 5 CHALLENGES OF PRESERVATION AND SECURITY OF LIBRARY AND INFORMATION SYSTEMS AND RESOURCES IN NIGERIA

CONTENTS

1.0 INTRODUCTION

Libraries and information centres take deliberate steps to protect their resources. In this regard, they provide special funds for the preservation and security of library items. However, the journey towards preservation of library items is not an easy one. Most often, the librarian and the management of the institution are confronted by daunting challenges in efforts to secure library materials and resources. In this unit, we will be discussing the challenges of preservation and security of library and information systems and resources particularly in Nigeria. It will be interesting to discuss possible ways of tackling the naughty challenges face library and information centres in Nigeria in the fight against the destruction of library items.

2.0 INTENDED LEARNING OUTCOMES (ILOs)

By the end of this unit, you should be able to:

i. explain the general perspective in the arduous tasks of preservation and security of library and information systems and resources.

ii. determine the challenges in handling Information Systems (IS).
iii. ascertain ways to tackle the challenges that face librarians in preservation of information resources and systems

3.0 MAIN CONTENT

3.1 Preservation and security of library and information systems and resources

Several studies have shown that there are several and peculiar challenges facing library and information centres in Nigeria and other developing countries in general. In other words, numerous issues impede the workability of the libraries as an institution, on one hand and its service provision on the other. These issues as well have hindered the security embroiled in the preservation of library resources to prevent them from damage and deterioration. In all, the inability to provide lasting solution to these problems have deterred the library from working to its full capacity as well as undermining the service provision.

Libraries as a store house of knowledge and information must be safe from security threats and vulnerability of its resources. Library collections which support the users' community through access to its collections are broad and varied. The access and use of library resources serve as privileges which provide important means of giving users the library's collections for personal, educational, and socio-economic advancement. Gelfand (2005) posits that the library is the only centralized location where new and emerging information technologies can be combined with knowledge resources in a user-focused, service, rich environment that support today's social and educational patterns of learning, teaching and research.

Library services can only be achieved through the availability of library resources and services. Unfortunately, libraries are faced with hybrid challenges of managing resources as well as the challenge of acquiring the necessary devices and skills needed for adequate security of the materials/resources both in print and electronic format. Chaney and MacDougail (2004) state that information resources in the library are vulnerable to abuse of one sort or another and library managers need to keep this characteristic well to the forefront of the library. Ensuring effective use, longevity and accessibility of library resources makes an effective programme of security of the collections necessary.

Antiwi (2009) also states that book theft (stealing of books) was already a great challenge to the libraries even at the beginning of library existence. Historically, book theft is believed to have started when the Persians went to Egypt and with one word drew papyrus from the Library of Ramses II without stopping for any formalities at the charging desk. They thus began this illegal practice which has continued to torment libraries ever since (Antiwi, 2009). The aim of gaining access and using information

resources in the library is to support the mission of the institution and to achieve this, it is imperative to ensure the safety and security of both print and digital collections in the library.

Therefore, the act of securing information resources in the library can be termed as a deliberate process to protect it from theft or loss, unauthorised access, disaster and well as from intruders. It can also be referred to as the way information security policies, programmes, measures, and procedures are deployed to protect library resources to enhance users' access and use.

Nevertheless, digitalization of library resources has brought about the evolution of cybersecurity risks, priorities, and resources. It has also led libraries to adapt to give an accurate snapshot of cybersecurity procedures taken by other organisations to protect the available resources. It is surprising to note that while ICT and the digital library has brought immense information access and utilization benefits to the users, t the consequent cyber risks seem to have rapidly eroded its benefits. Libraries that rank low on ICT applications are the ones in the least developed countries with more print than digital resources. The truth is: are these libraries in developing countries with low ICT penetration not faced with the same preservation and security challenges? As more libraries in these countries begin to become more connected, they would need support to develop cybersecurity capacity to better respond to threats. But, the challenges of digital preservation and cybersecurity are continually evolving in behaviour, and practices.

Information security, also known as InfoSec, is an exercise of protecting information resources and information-bearing materials from unapproved access, use, disclosure, recording, modification, perusal, disruption, inspection, or destruction. You can as well use the term *infosec* notwithstanding the form the data may take. The definitions of InfoSec suggested in different sources are summarized below:

v. Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009).
vi. The protection of information bearing materials i.e., book and non-book materials and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability." (CNSS, 2010).
vii. The assurance that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008).
viii. Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000).

ix. Information security is the protection of information, information bearing materials and the minimizing of the risk of exposing information to unauthorized parties." (Venter & Eloff, 2003)

Lots of libraries have digitalised while some are in the route of digitalising both in the collections and service provision because of ICT advancement. Despites the advantages of 'going digital', the fact remains that several basic issues vis-à-vis the long-term preservation of digital library resources remain unresolved. Kademani, Kalyane and Kumar (2003) argue that the two key problems are the fragility of digital media (its 'shelf life' compared with, say, non-acidic paper is extremely short) and, perhaps even more intractable, is the rate at which computer hardware and software become obsolete. In many occasions, vital data/information have been lost due to outmodedness while long term preservation of some digital library materials such as multimedia documents have been problematic even till this day.

Preservation and conservation of library materials and other information systems have become a global issue which must be tackled if the mission of providing library services and attainment of the vision of the library must be reached. Libraries, in general terms, acquire materials to meet the information need of the users. Ordinarily, library and information systems and materials deteriorate or are damaged due to several factors such as natural and man-made disasters, change in chemical composition of the materials, as well as vulnerability to security threats etc. As a result, it is the responsibility of the librarians to keep these materials and the information systems in good condition.

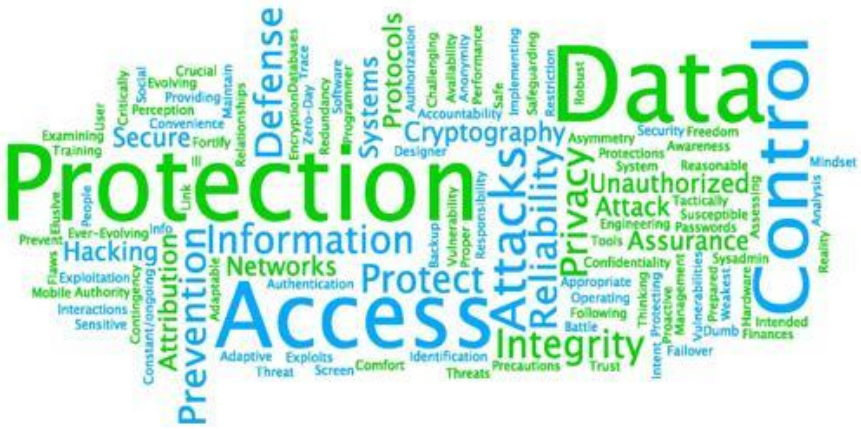
Unfortunately, the sad situation of deterioration of information-bearing materials in the library has a long history in Nigeria. For instance, most library materials (print and non-print) in Nigeria are still housed in conditions that are prone to deterioration and security risk. According to Popoola (2003), a large portion of the information recorded on audio or videotape about important events, people etc, have been routinely wiped out in our electronic media houses. To this end, unless urgent and proactive measures and actions are taken to guide against it, library materials will continue to deteriorate. It is worth to note that the process of protecting or preventing library materials including intellectual heritage from deterioration is a battle to be waged by the librarians and other well-meaning information professionals.

Preservation and conservation of library materials involve the act of preserving, protecting and shielding materials from destructive impacts that may shorten the life span of the materials as well as guiding against loss.

3.2 Information System (IS) and its Challenges in Nigeria

The Information System (IS) like any other information structure is aimed at turning raw data into useful information that guide in decision making. This is a combination of the corresponding network of apparatuses which act together to produce, distribute and process information. The information system is characterised by a computer-based information system. Similarly, an information system may be referred to as organisational. sociotechnical, formal system that are designed to gather, process, store and disseminate information.

In other words, each of these systems outlined above work together to support the information system in institutions or organisations to achieve desired goals. The sociotechnical system comprises four components namely: task, people, structure and role. Furthermore, the main components of the information system include telecommunication, computer hardware and software, human resources, procedures, databases, and data warehouses. Some of the information system components such as computer hardware and software as well as telecommunications constitute information technology (IT) which are embedded in the operation and management of organisations or institutions.



Issues in Information systems. pt.slideshare.ne

3.2.1 Components of Information System

The Information System is made up of the following elements:

Telecommunication: This is communication that uses various types of technologies through wire, radio, optical and other electromagnetic system over a long distance that is faster than the postal mailing system. According to Idris (2010), telecommunication refers to the transfer of data (communications) from a transmitter to a receiver across a distance. Data/code represented by some form of electromagnetic energy – electricity, radio waves, lights – transmitted through medium- wire, cable, and atmosphere. In other words, it is a communication over a long distance (tele = far off). It can also be referred to as any communication in the form of transmission, emission, receiving and sending of signs,

signals, writings, sound, images or intelligence via electromagnetic systems or wire, radio and optical elements. The components of telecommunication system include:

* Transmission equipment
* Switching equipment
* Terminal equipment and
* Support system

Telecommunication system www.ocean-ops.org

Computer hardware and software: A computer software is a gathering of instructions that define an assignment, or set of assignments, to be carried out by a computer. It gives instructions that control the working of the computer system. It is the collection of programming codes installed on your computer's hard drive. Whereas hardware is the computer components you can hold in your hand. This means that while you can touch or hold the hardware, the software cannot be held in your hand.

Computer hardware www.chtips.com

Human resources: An asset and the workforce of any organisation in the form of human capital, knowledge and skills that every individual worker possesses. On the other hand, human resources management involves the development and administration of plans designed to increase and improve efficiency and effectiveness of an organisation via the personnel. It also includes the whole range of creating, cultivating, and managing workers-management relationship aimed at enhancing productivity and harmonious work environment.

Human resources www.thebalancecareers.com

Procedures: An established way of doing certain things especially in a formal organisation. In other words, it is the sequential actions or designs to accomplish tasks. In computer programming, a procedure is a set of coded instructions that tell a computer how to run a program or calculation. Many different types of programming languages build a

procedure. Depending on the programming language, a procedure may also be called a subroutine, subprogram or function (ComputerHope, 2017).

Data warehousing: Data warehousing is the central storehouses of combined data from one or more distinct sources. Data warehousing stores both current and historical data/information in one single place that are used for creating analytical reports that help in decision making.

Data Warehousing: www.astera.com

Databases: It is an organised collection of data stored and accessed electronically from a computer. Generally, **i**nformation system databases are more complex, because they are often designed using formal strategy and modelling techniques. Database, also known as electronic database, is any collection of data/information that is organised specially for rapid search and retrieval by a computer. It is designed to aid the storage, retrieval, modification, and removal of data in conjunction with several data-processing operation.

Information System Database:
https://slideplayer.com/slide/6895010/

3.2.2 Challenges of Information Systems

New skills: There is a need for a set of skills that are different while developing information systems. Fresh types of skills are required to buttress emerging information systems, and these are lacking in Nigeria and other African countries. Systems experts and program writers are no longer an appropriate separating of "workers" in a development project. Hence, identifying these skills as well as providing them with adequate training has proven a major challenge.

Methods and techniques: Most of the methods and techniques used in developing information systems hardly provide solutions to the issues at hand. As a result, most research methods deal with development (or re-development) of formal description techniques with a high expressive power for describing things which can be formally described.

Informality: Nowadays, countless ICT development projects deal with engineering or re-engineering of corporate processes and providing adequate IT-support for the processes which is characterised by casual or ordinary use.

Maintenance: Major challenges for management information systems is providing the raw data input and the maintenance or upkeep of up-to-date information. An organisation or institution most often finds it difficult to manage and maintain an already generated data on sales, revenues, expenses, payments and other fundamental business information, in addition to other departments which often have additional databases.

Use: Ability to use an already generated data most times pose a great challenge. Therefore, the organisation's generated data becomes useless if it is not utilised by the personnel

***Changes*:** Time, personnel, and the need for data always change. Therefore, it is important that the management of an information system should exhibit the characteristic of flexibility and be ready to adapt to changes when the need arises. In other words, the availability of information may change, the reports may vary and at times the persons using the system may also change

3.3 Challenges of preservation and security of library resources in Nigeria

Like other related matters in the management of libraries and information resources, there are obvious challenges confronting the preservation of information resources and the smooth operation in service provision in the library. According to Sithole (2007), African libraries and information centres are faced with overabundance of issues in the preservation of library materials, documentation and communication of (indigenous) knowledge. This includes the lack of funds/resources, low human capacity development, technology shortages and the lack of legal frameworks at national and international levels to support the library efforts to document and communicate indigenous knowledge. The fast-developing information and communication technologies continue to pose challenges on how best libraries can document and disseminate ……. knowledge globally.

In general terms, most people consider the security associated with a system as they guard against theft and intentional destruction of properties. However, security in libraries involves the planning and policy of protecting its resources for effective service provision and posterity. Ordinarily, formidable procedures, plans and policies of security must revolve around tackling man-made disasters such as war, fire, theft/stealing, mutilation, dog ear, etc as well as natural disasters which include flood, earthquake, tsunami, volcano and hurricane etc. This means that the failure of security measures in and around the library premises obviously will result in the loss of valuable resources and the decline in the provision of quality services to the clients.

Also, Omosekejimi, Ijiekhuamhen, Ojeme (2015), stated the major issues confronting preservation and security of information resources and library materials to include:

1. **Insufficient funds:** In Nigeria, libraries and information centre's lack the funds to buy and install the telecommunication security systems that can help to safeguard the level of security required as a result of the low budgetary allocations from their parent body.
2. **Lack of skilled personnel**: Most Nigerian libraries and information centres lack expertise staff that can operate, impart and instruct the use of telecommunication security systems even when they are made available in the library.
3. **Inadequate or absence of electricity supply**: No telecommunication gadget can function without power supply. Hence, telecommunication security systems or devices require electricity to power them but due to the poor power supply, these systems often time do not work and as such are incapable of performing their expected tasks of securing the library and its collections.

4. **Hardware and software failure**: Failure in hardware and software forms major issues in the preservation and security of library resources. For instance, the information system and library information bearing-devices are at risk once there is software or hardware breakdown. This may involve the need for an expert who may not be readily available to attend to the quickly.
5. Libraries in remote areas do not have access to telecommunication security systems because they may not afford the huge financial investment required to acquire and install the necessary devices and adequately cater for them.

Mahapatra and Chatevabarti (2003) listed some of challenges that constitute substantial threats to library documents to include:

1. Deterioration of information resources because of natural age of paper since the major components are of organic nature. To improve on this, proper housekeeping should be in place.
2. The use of fibre with either low cellulose contents or sometimes non-cellulose materials of the lignin type makes paper degenerate easily.
3. Minerals and chemicals used as basic ingredients of paper affects its durability.
4. Impurities in the ingredients used as basic components of paper cause inevitable deterioration.
5. Acidic sizing materials such as alum, rosin etc in the paper manufacturing causes acidic effects.
6. Oxidizing agents make weakens paper, and cause discolouration and disintegration.
7. Presence of metals accelerate oxidation.
8. Fungi grows easily on paper made with alkalis.
9. Heat and exposure to sun make paper brittle and fade in colour.
10. Dust and particles cause paper discolouration and invites chemical change which encourages biological growth.
11. Some acidic elements such as sulphuric acid from dioxide in the atmosphere causes discolouration and disintegration of paper.
12. Moisture and humidity create biological attack on paper.
13. Non-print materials such as films are very sensitive to excessive heat, dryness, moisture and humidity.
14. Chemical present in audio/visual materials can cause deterioration especially under harsh atmospheric condition.

In addition to the already mentioned challenges, studies have also shown that the following are the key challenges to preservation and security of library information resources:

- **Budget cuts:** The challenge of budget cuts arise as result of reduction in the budgetary expenditure and allocation for library

upkeep by the parent body or institution. There are signs of economic melt-down in Nigeria and some other developing countries, resulting to the nation's reduction in budgetary allocation to several segments of the economy. This in turn affects other substructure of the economy such education where the library falls under.

- **Changes in technology:** The world-over have witnessed a tremendous technological advancement because of inventions, innovations, and developments in the overall technological processes. The emerging technology in areas of diffusion, processes, research and development has brought changes in technology, that is less expensive and more commercialized than before. Similarly, changes in technology have become more of a challenge than a gain among the libraries in Nigeria for the fact that most libraries have been unable to catch-up with the emerging trends in the ever-improving technology. In fact, these libraries are lagging in catching up with changes in technology.
- **Changes in people's lifestyles:**

  Several changes have taken place within the past decades. These changes have affected peoples' lifestyles such as standard of living, means of communication, urbanization as well as educational processes etc. Consequently, people's preferences have also changed and one of such changes has to do with carrier and education. Lately, the experience of the global Covid-19 epidemic has exposed the new ways of carrying out normal businesses (The New Normal).

Changing lifestyle: https://www.apa.org

In practice, libraries have lost most of its customers partly due to the Covid-19 pandemic and the digital boom which created the new ways of sourcing information other than going physically to the library.

- **Preservation and deterioration:** The preservation of library materials is one of the core responsibilities of librarians. According to the Encyclopaedia of Communication and Information (2002), 'preservation involves maintaining an object or information in a format that the continued use and accessibility of information is guaranteed. It includes developing the criteria for selecting materials that have cultural or historical importance and assessing their preservation needs; halting the deterioration of materials by providing a stable environment and proper supplies and equipment for storage; developing and providing the resources necessary to engage in an on-going preservation program committed to the continued existence of valued materials by providing a stable environment and proper implementing policies for the safe use of materials; and providing the resources necessary to engage in an on-going preservation program committed to the continued existence of valued materials.

  Preservation also includes preparing for potential disasters such as floods, fires, tornadoes, and earthquakes. Conservation is to stabilize and restore an object in its original form through various treatment methods. Professional conservators are trained to apply conservation treatment methods and move recommendations for long-term preservation of materials in suitable environments (Mundi 2017).

  On the other hand, deterioration is a state of decrease in value. In library, deterioration entails the depreciation of library materials in value and quality. Arguably, deterioration starts the very moment a material is invented, or a book is published. Most times deterioration come about because of the materials used in making either the print or non-print items in the library. It could be due to natural causes such as moisture, dryness, acid, alkalis, dust, heat ultra-violet radiation, cold etc. It can as well be caused by chemical reactions because of the materials used in its production.

  Moreso, deterioration can be caused by biological elements such as insects, fungi, bacteria, etc. The cause of deterioration, in general terms, can be classified into chemical, physical, environmental, and biological factors which aid in degeneration, aging and decaying of library materials.

Ebijuwa, Ogunimo, Adefunke (2013) highlighted the following challenges facing preservation and security of library material in Africa:

- **Inadequate equipment:** Most of the equipment and materials needed for preserving and conserving library materials are lacking in most libraries in Africa.
- **Tropical climate condition:** The African tropical climate, excessive heat and temperature, relative humidity as well as rodents that feed on paper contribute in no small measure to the deterioration of library materials in Africa.
- **Lack of manpower and training:** No reasonable or meaningful preservation and conservation activity can take place without a trained manpower with sound technical know-how to handle them. Hence, there is the lack of manpower to handle preservation and conversation of library materials whereas the available personnel in the library hardly get adequate and regular training. Also, training of librarians is almost absence.
- **No preservation and conservation policies in place:** Policies are plans, procedures and strategies that guide actions. Most libraries in Africa do not have preservation and conversation policies in place, while those that have do not adhere to such.
- **Low quality of paper and ink used in publishing:** Some of the constituents used in the paper manufacturing and book publishing in Africa are usually fake and below international standards and this affect the durability and longevity of the library resources especially the print materials
- **Maintenance culture:** Maintenance is the act of preserving, conserving and upkeep of materials to retain definite forms, values and standards. Unfortunately, just like in the larger African systems, library managements lack good maintenance culture that will keep library materials in good condition for long period of time.
- **Administrative problem:** A good administration enhances smooth running of an institution or organisation, but lack of it always brings malfunction, breakdown and failure in the implementation of programs and policies. Most libraries in Africa lack good administrators and administration.
- **Cooperative preservation and conservation venture:** In Africa, there is no local or regional joint ventures where librarians and libraries pull their resources together to fight against deterioration and promote library materials preservation and conservation.

3.3.1 Agents of deterioration of library materials

Several factors are involved in the deterioration of library materials, nevertheless, some measures can be taken either to avoid deterioration or to minimize its effects on the library materials.

1. **Chemical Agents:**
   Substances like sulphur dioxide, oxides, nitrogen, and ozone are toxic elements which are used in the production of paper materials are hazard to cellulose materials such as paper and cloth. Hence, fibres, cellulose contents and some chemical compound like alum, rosin are used in paper production which cause acidic effect on the paper and promote deterioration with the passage of time. In addition, the atmosphere contains some elements such as oxides of carbon, sulphur, nitrogen and hydrogen sulphides and these can cause deterioration when absorbed by paper materials

Chemical substance: www.umweltbundesamt.de

Chemical agents include:

- Dust and dirt
- Internal acidity of paper and ink
- Air pollution and
- Atmospheric gases

Preventive measures of Chemical factors

Pollution control will help to reduce any external acidity on the library materials. Filtering of the air intake into storing zones, which can be achieved by functional air conditioning systems is considered one of the best ways of controlling atmospheric pollutants in the library. Other measures such as rapping of books in cloth materials and placing them in containers is another option for preserving library materials. Logically, books kept inside are better protected than the ones outside.

If adequate care is taken to save books and documents from dust, then the use of vacuum cleaners to clear dust and dirt is preferable. The use of

chemical formulation directly on the books should be avoided because of its adverse effects on the materials, personnel and clients. The use of wooden storage should be avoided unless it is covered with coats of acrylic emulsion paint. Further, the use of good quality materials, acid free paper and board ought to be encouraged for repairing and restoring documents

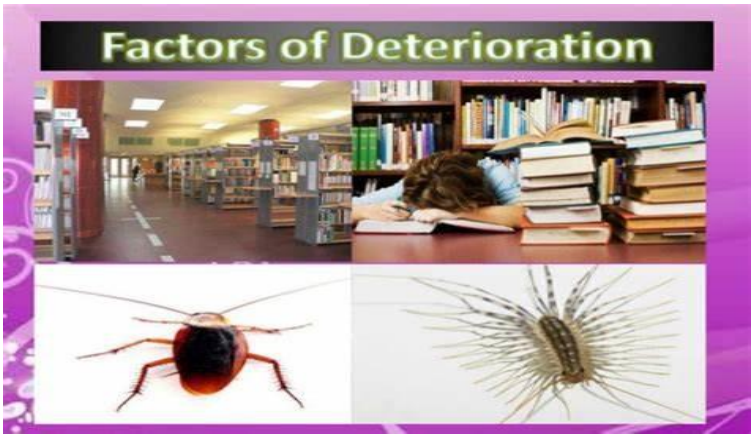
2. Biological Agents

Some biological agents such as fungi, insects, moulds and rodents etc which cause deterioration and often increases the organic matter in the library, especially when a suitable, conducive and stable ventilation, lightening, temperature and humidity are not properly taken care of. The growth of these biological agents causes infection on the library materials. These biological agents can be grouped into micro and macro-organisms and each of these agents attack paper especially when the temperature and humidity are not controlled.

Biological agents

Macro organism

- Silver fish
- Book lice
- Book worm
- Cockroaches
- White ants (Termites)
- Rodents
- Beetle
- Man



Some macro organism: www.istockphoto.com

Micro organism

- Fungus
- Mildew
- Mold

Books affected by some micro-organisms:
www.nationalgeographic.com

Preventive measures for Biological factors

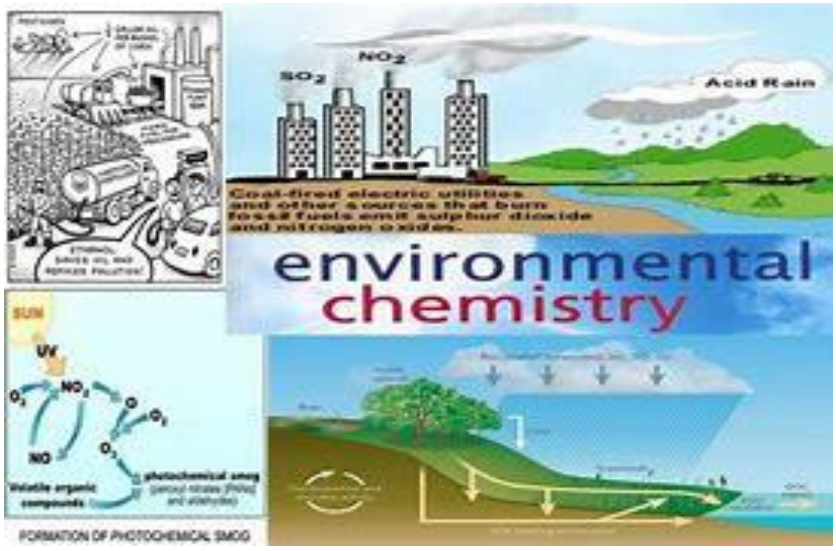
Air stagnation, darkness, wetness, and dirty places within a library enables the growth of biological pests. Therefore, a good housekeeping and maintenance of optimum storage condition is necessary for controlling the propagation of the insects. Also, providing ventilators, cross-windows and exhaust fans warrant good circulation of air. It is also essential to circulate the air inside the room with electric fans. To reduce dampness, book racks should not be placed close to the wall (at least 15cm away from the wall)

Constant maintenance of broken and cracked walls, floor, and loosed building joints will help to reduce or eliminate possible insects in the building. The cracked and broken building partitions provide hiding places for insects. Foods or other edibles should not be allowed into the library because they attract insects. Insecticide powers like lindane, almirahs and paradichloro-benzens should be use or placed at every corner of the library to ward off and prevent insect attacks. Another simple method is keeping naphthalene bricks on the bookshelves to prevent insects which attack library materials from entering the library building to create havoc. The use of dry leaves and seed powder and camphor tablets should be kept inside the racks for preventing insects from entering the shelves and the library building.

3. Environmental Agents

Materials of organic origin such as leather, parchment and artefacts in which cellulose fibres such as paper products form the support likely to be soiled and stained by solid particles of carbon, tarry matters and other solid contaminants. The worse contaminants for this group of materials are sulphurous and sulfuric acids resulting from the combustion of fuels and from other industrial processes. The effects are severe with cellulose

materials such as paper and leather. There is a close correlation between the loss of strength of paper and its acidity resulting from sulfuric acid contamination. Dust and dirt particles in the air not only carry with them the adsorbed pollutants but may exert an abrasive action on books and paper (Mahmood & Mari 2013).



Agents of environmental factor: **Source:** environmentalhealth.ucdavis.org

- Temperature
- Relative Humidity
- Light
- Atmospheric pollutants
- Water

Environmental pollution: www.niehs.nih.gov

Fast and severe weakening of paper is caused by the oxidation of cellulose as a result of ultraviolet rays in sunlight and fluorescent light. The effects of light and other atmospheric pollutants on paper or other print materials in the library are noticeable namely, it leads to the bleaching action that causes some whitening of paper and fading of colours and inks used in printing of paper. Also, the atmospheric light or pollutants cause lignin (amorphous polymer used in paper production) to turn paper to yellowish or brownish colour especially when exposed with other compound used in paper production.

Preventive measures for environmental factors

The prevention of environmental factors partly begins from selecting, planning and constructing site and the library building. Consideration should be made on the soil texture on which the library building will be constructed because these elements have greater impacts over the environmental regulator inside the library building. It is very essential in selecting the best architectural design for the library at least to have a cross ventilation facilities for free air passage within the building. If there is a need to use wooden materials, then, it is better to use seasoned wood which would be treated with chemical substance to avoid infection of insects. Planting and growing of big trees within the surrounding of the library build should be avoided, to avoid its root from damaging the building foundation.

In order to prevent dust and dirt to affect library materials, it is also always better that the library building should be constructed away from the traffic. Providing enough electric fans and few exhaust fans will ease air circulation inside the library. The sun is a great emitter of ultraviolet rays. Therefore, direct sunlight should be prevented from falling on papers. Also, the windows must be provided with coloured curtains, which will avert dropping of direct light as well as absorbing infrared waves. Glass panes with colours such as yellow, green or lemon must be fitted in windowpanes. These colours are more effective in obstructing ultraviolet rays. It is very good fitting acrylic plastic sheets in the windowpane for the fact that it filters out ultraviolet rays to a greater extent than coloured glasses.

It is good to filter ultraviolet rays from fluorescent tubes by covering the tubes. It is wise to maintain an ideal room temperature of about (200-250 c) as well as relative humidity of (RH 45-55%) for preservation. This is because a high temperature and high humidity are hazardous to the library materials. To maintain ideal temperature and humidity, air conditioning of the stack area is mandatory for storage of library materials. Obviously, provision of round-the-clock air conditioning may not be feasible for most libraries in Nigeria. Therefore, local control measures of maintaining a balanced humidity and temperature as well as the use of humidifier in dry climate to get a favourable climate. Sohoo (2004) maintains that these may be operated whenever necessary for proper monitoring of relative

humidity. High humidity could also be minimized using de-hydrating agents like silica gel. The requisite quantities of silica gel may be spread in dishes and kept in different places in the room. After the use for 3-4 hours the silica gel may get saturated and may need replacement with fresh gels, while the saturated gel can be reactivated for further use after heating it in open pans.

In summer periods, temperatures are usually high. Therefore, the windows should be kept shut or the wet curtain should be used if the windows should be opened. To maintain free air circulation, high-speed air conditioners should be used as well. Wet duster should be used to clean the floor of the library building. Too much of dust and dirt increase the physical damage of books. Thus, maintaining a cleaning schedule should be made bearing in mind the sequence of operations following daily and weekly practices. The use of vacuum cleaners to suck the dust and dirt from inner corners of staking stakes and shelves and other dust accumulating surfaces.

4. Natural Agents

Ordinarily, natural disasters are very difficult to predict. Most times they occur without noticeable signs or warning. Hence, librarians should include contingency plans in their preservation policy program to minimise, prevent or reduce the impact of occurrence as well as to rescue materials in cases of eventuality or disaster strikes. It is very difficult to predict the natural disasters. Therefore, there should be a contingency plan which should form part of the preservation policy aimed at minimizing loses and rescuing materials to safer places when disasters strike.

There should be installation of vital equipment such as firefighting apparatus, security monitoring gadgets etc, in and around the library. In addition, there should be constant security briefing, updates, drilling and training of the personnel.

Atmospheric mechanism: pubs.rsc.org

Agents of natural factor

- Flood
- Earthquake
- Tsunami
- Volcanoes
- Hurricane

Preventive measures of natural factors

Natural factors are usually disasters which are unexpected disruptive events and occurrences that befall the library collections, buildings or surroundings. Thus, it is important for libraries and librarians to take adequate precautionary measures to prevent the avoidable ones and adopt good response mechanisms to the possible occurrences.

The availability of disaster management plans and strategies become the main key to prevent conservation. It will as well provide a means for easy identification of both internal and external threats to the materials. Disaster plans serve as a preparedness strategy for crises management to meet the perceived threats without which it will be difficult to salvage disaster situation in a good time.

It should be required for every library to have a written disaster preparedness and response plan containing description of emergency procedures, emergency supplies list, disaster response outline, conservation experts, list of staff volunteers, list of external contacts and names, addresses, home and work telephone numbers of personnel with emergency responsibilities.

In addition, libraries should be provided with fire and smoke detection systems and automatic fire extinguishing systems. Use of flammables, pets, toddlers, matchsticks or open flame and smoking should strictly be prohibited inside the library. A muster point should clearly be marked. Chemical substances should not be stored inside the stacks within the premises of the library. Leaking roofs and facilities such as gutters should be adequately taken care of. The telephone numbers of the Department of Fire Service and other emergency agents should be stated and clearly written for easy access and use. Regular repairs and fixing mechanism of electrical faults should be put in place

5. Human Agents

Part of the environmental, chemical and biological factors of deterioration are directly or indirectly caused by human attitudes, actions or inactions toward the library materials. The librarians who are the custodians of library and information resources and charged with the responsibility of the overall preservation and conservation of the materials often fall short in these tasks. Mostly, the techniques of material handling in the area of transportation, photocopying, exhibition and storage system often expose the materials to deterioration. On the other hand, library users sometimes exhibit very low standard of care and handling of books. Some users intentionally rough handle materials by marking by pens, dog ear, mutilation and even steal these materials.

Human factor: Source: www.shutterstock.com

Agents of human agents

- Fire
- Theft and vandalism
- Material handling (transportation, photocopying, exhibition and storage system)
- Mutilation

3.3.2 Preventive measures for human agents

There are procedures, plans and strategies librarians as well as library users should take to maintain and increase the longevity of the library resources. These include among others:

- Important books and manuscripts should be kept in specially prepared containers.
- For carrying many books, trolleys should be used. Utmost care should be taken while transporting rare, valuable and delicate books.
- Care should be taken while photocopying the books because considerable stress may be exerted on the material and the bindings suffer the most and also the spines might be affected too.
- Use bookends to support books when shelves are not full. Books should not be shelved too tightly or too loosely.
- It must always be ensured that while opening the books, pages are not torn or covers damaged. To turn a page, lift the top corner and lightly slip the fingertips down the fore-edge supporting the page.
- Pages should never be folded otherwise creases will be formed and they may be torn at the folds. Corner of pages should not be folded to mark pages.
- Avoid licking of fingers as an aid to turn pages.
- Underlining must be avoided.
- Books should not be left open on the reading table, face downwards.
- Leaning on an open book should be avoided since this can damage the spine and binding.
- Never allow a book to stand on its fore edge.
- When a book is displayed open, never use metal clips or pins to hold book pages open (Mahmood & Mari 2013).

4.0 CONCLUSION

In this unit, we have navigated through various issues relating to challenges faced by the libraries especially in Africa. It is worth noting that if streamlined and proactive actions in not taken, the provision of lasting solutions to challenges affecting the libraries and the attainment of improved library service provision, the preservation of information resources and smooth running of the libraries will continue to be a mirage.

5.0 SUMMARY

In Nigeria and generally all-around Africa, there are challenges of preservation and security of library and information systems and resources. Our discussion in this unit focused on the following thus:

- Preservation and security of library and information systems and resources
- Information System (IS) and its Challenges in Nigeria
- Components of information system
- Challenges of preservation and security of library resources in Nigeria
- Causes of deterioration of library materials and
- Preventive measure for deterioration

6.0 TUTOR-MARKED ASSIGNMENT (TMA)

1. List and explain the components of an information system as discussed in this unit
2. Define deterioration and lift the agents responsible for deterioration of library materials
3. List and explain the major issues confronting the preservation of library materials in Africa according to Omosekejimi, Ijiekhuamhen, Ojeme (2015)

7.0 REFERENCES AND FURTHER READING

Antiwi, I. K. (2009). The problem of library security. The Bauchi Library experiences International Review. *Journal of Academic Librarianship*. 21:363-372.

Chaney, M. & MacDougail, A. F. (2004) *Security and crime in libraries*. Gower Publishing.

CNSS (2010). Implementing a CNSS 4012 certification on an information. Retrieved from: https://www.uttyler.edu/cs/documents/subramanian_whitson.pdf

ComputerHope (2017) What's Happening @ LWLC: Computer Learning Month. Retrieved from:

Gelfand (2005). A Conceptual Approach to the Role of the Library in Developing Countries. Education Libraries Journal. 40 (3): 13-22.

Gregersen, E. (nd) Components of Information Systems. Retrieved from: https://www.britannica.com/list/5-components-of-information-systems (May 2021)

https://alasu.libguides.com/c.php?g=726667&p=5187278 (May 2021)

ISACA, (2008). Storage area networking security devices. Retrieved from: https://www.sciencedirect.com/topics/computer-science/information-systems- audit-and- control-association

ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/standard/41933.html

Kademani , B. S., Kalyane, V. L & Vijai, K. B. (2003) Preservation of information resources in Libraries : New Challenges .Retrieved from rclis.org (8th May 2021)

Mahapatra, P. K & Chakrabarti, B. (2003). P*reservation in libraries: Perspectives, principles and practice*. New Delhi: ESS Publication

Mahood, Z. U., & Mari, H. M. (2013) Deterioration of library resources and its causes: Theoretical review. Retrieved from https://citeseerx.ist.psu.edu/ (August 2021).

Mundi, S. (2017) Preservation and conservation of library materials: a practical hint Retrieved from https://nji.gov.ng (10th February 2021)

Ogunmodede, T. A., & Ebijuwa, A. S. (2013). Problems of conservation and preservation of library resources in African Academic Libraries: A review of literature. Retrieved from: https://www.academia.edu/22943392/

Pipkin, D. L. (2000). *Information security: Protecting the global enterprise.* Retrieved from:*https://books.google.com.ng/books/about/Information_Security.html?id= HTt kQgA ACAAJ&redir_esc=y*

Popoola, S. O. (2003). Preservation and conservation of information resources. University of Ibadan, Nigeria: Distance Leaving Centre.

Schement, J. R. (2002). Encyclopaedia of communication and information. Retrieved from: https://www.worldcat.org/title/

Sithole, J. (2007).The challenges faced by African libraries and information centres in documenting and preserving indigenous knowledge Accessed from: https://journals.sagepub.com/doi/abs/ (November, 2021)

Venter, H. & Eloff, J. (203). A taxonomy for information security technologies. Retrieved from: https://www.semanticscholar.org/paper/A-taxonomy-for-information- security-technologies